S. HRG. 106–885

ID THEFT: WHEN BAD THINGS HAPPEN TO YOUR GOOD NAME

HEARING

BEFORE THE

SUBCOMMITTEE ON TECHNOLOGY, TERRORISM, AND GOVERNMENT INFORMATION

OF THE

COMMITTEE ON THE JUDICIARY UNITED STATES SENATE

ONE HUNDRED SIXTH CONGRESS

SECOND SESSION

ON

EXAMINING THE EFFECTIVENESS AND FUNDING FOR THE IDENTITY THEFT AND ASSUMPTION DETERRENCE ACT (P.L. 105–318)

MARCH 7, 2000

Serial No. J–106–70

Printed for the use of the Committee on the Judiciary

U.S. GOVERNMENT PRINTING OFFICE
69–821 CC WASHINGTON : 2001

COMMITTEE ON THE JUDICIARY

ORRIN G. HATCH, Utah, *Chairman*

STROM THURMOND, South Carolina	PATRICK J. LEAHY, Vermont
CHARLES E. GRASSLEY, Iowa	EDWARD M. KENNEDY, Massachusetts
ARLEN SPECTER, Pennsylvania	JOSEPH R. BIDEN, JR., Delaware
JON KYL, Arizona	HERBERT KOHL, Wisconsin
MIKE DEWINE, Ohio	DIANNE FEINSTEIN, California
JOHN ASHCROFT, Missouri	RUSSELL D. FEINGOLD, Wisconsin
SPENCER ABRAHAM, Michigan	ROBERT G. TORRICELLI, New Jersey
JEFF SESSIONS, Alabama	CHARLES E. SCHUMER, New York
BOB SMITH, New Hampshire	

MANUS COONEY, *Chief Counsel and Staff Director*
BRUCE A. COHEN, *Minority Chief Counsel*

SUBCOMMITTEE ON TECHNOLOGY, TERRORISM, AND GOVERNMENT INFORMATION

JON KYL, Arizona, *Chairman*

ORRIN G. HATCH, Utah	DIANNE FEINSTEIN, California
CHARLES E. GRASSLEY, Iowa	JOSEPH R. BIDEN, JR., Delaware
MIKE DEWINE, Ohio	HERBERT KOHL, Wisconsin

STEPHEN HIGGINS, *Chief Counsel and Staff Director*
NEIL QUINTER, *Minority Chief Counsel and Staff Director*

CONTENTS

STATEMENTS OF COMMITTEE MEMBERS

CHRONOLOGICAL LIST OF WITNESSES

ALPHABETICAL LIST AND MATERIAL SUBMITTED

APPENDIX

QUESTIONS AND ANSWERS

ID THEFT: WHEN BAD THINGS HAPPEN TO YOUR GOOD NAME

TUESDAY, MARCH 7, 2000

U.S. SENATE,
SUBCOMMITTEE ON TECHNOLOGY, TERRORISM,
AND GOVERNMENT INFORMATION,
COMMITTEE ON THE JUDICIARY,
Washington, DC.

The subcommittee met, pursuant to notice, at 2:06 p.m., in room SD–226, Dirksen Senate Office Building, Hon. Jon Kyl (chairman of the subcommittee) presiding.

Also present: Senator Grassley.

OPENING STATEMENT OF HON. JON KYL, A U.S. SENATOR FROM THE STATE OF ARIZONA

Senator KYL. Good afternoon. This hearing before the Senate Committee on Judiciary Subcommittee on Technology, Terrorism, and Government Information will please come to order. The subject of today's hearing is "ID Theft: When Bad Things Happen to Your Good Name." I welcome all of you to the hearing.

I will begin by indicating that Senator Feinstein is in her State of California because of her State's primary and therefore will not be joining us today. There may be other members of the panel, however, either on the Democrat or Republican side, joining us as the hearing progresses.

There are some statements that I will put into the record at the very beginning. Senator Patrick Leahy has a statement for the record.

[The prepared statement of Senator Leahy follows:]

PREPARED STATEMENT OF SENATOR PATRICK J. LEAHY

Less than two years ago, President Clinton signed the "Identity Theft and Assumption Deterrence Act of 1998" into law to crack down on the theft of another person's identification information that results in harm to the person whose identification is stolen and then used for false credit cards, fraudulent loans or for other illegal purposes. This new law also set up a "clearinghouse" at the Federal Trade Commission to keep track of consumer complaints of identity theft and provide information to victims of this crime on how to deal with its aftermath.

This law was the product of bipartisan concern and good faith efforts to develop a legislative response to the growing problem of identity theft. I am proud of the work Chairman Kyl, Senator Feinstein and I, and others, did together to produce a strong, effective law.

Protecting the privacy of our personal information is a challenge, especially in this information age. Every time we obtain or use a credit card, place a toll-free phone call, surf the Internet, get a driver's license, or go shopping online, we are leaving virtual pieces of ourselves in the form of personal information, which can be used without our consent or even our knowledge. Too frequently, criminals are getting

hold of this information and using, the personal information of innocent individuals to carry out other crimes.

The consequences of identity theft for its victims can be severe. These victims can have their credit ratings ruined and be unable to get credit cards, student loans, or mortgages. They can be hounded by creditors or collection agencies to repay debts they never incurred, but were obtained in their name, at their address, with their social security number or driver's license number. It can take months or even years, and agonizing effort, to clear their good names and correct their credit histories. I understand that, in some instances, victims of identity theft have even been arrested for crimes they never committed when the actual perpetrators provided law enforcement officials with assumed names.

The FTC has recently made available online a number of valuable resources for consumers and victims of identity theft. One such document, called "ID Theft: When Bad Things Happen to Your Good Name," contains poignant stories from consumers about how ID thieves have damaged their lives.

One consumer reported to the FTC that:

> "Someone used my Social Security number to get credit in my name. This has caused a lot of problems. I have been turned down for jobs, credit, and refinancing offers. This is stressful and embarrassing. I want to open my own business, but it may be impossible with this unresolved problem hanging over my head."

Yet another consumer reported:

> "My elderly parents are victims of credit fraud. We don't know what to do. Someone applied for credit cards in their name and charged nearly $20,000. Two of the card companies have cleared my parents's name, but the third has turned the account over to a collection agency. The agency doesn't believe Mom and Dad didn't authorize the account. What can we do to stop the debt collector?"

Identity theft is a problem that reaches into every state. One of my constituents had to deal with this problem several years ago. In June of 1997, on the night before her wedding, a woman stole Carla Chadwick's purse. Ms. Chadwick, a resident of Burlington, Vermont, canceled her credit cards and assumed that the story would end there. Unfortunately, this was just the beginning of her nightmare. For the next two years the thief assumed Ms. Chadwick's identity, and went on a cross-country spending spree, damaging Ms. Chadwick's credit along the way. The thief also checked into hospitals under Ms. Chadwick's name, and accrued thousands of dollars in medical charges. This thief even applied for welfare, again under Ms. Chadwick's name. Officials believe that, in total, the thief racked up more than $58,000 of fraudulent charges, all in Ms. Chadwick's good name.

The nightmare finally came to an end in December, 1999, when the thief, later identified as Carla Mae Purdy, was arrested in Spokane, Washington. Carla Mae Purdy now faces prosecution under the "Identity Theft and Assumption Deterrence Act of 1998," and Carla Chadwick can reclaim control of her good name.

Such stories abound across the nation, and the "Identity Theft and Assumption Deterrence Act" appears to be helping law enforcement catch and prosecute ID thieves. For example:

- In July, 1999, the United States Secret Service announced the indictment of Terkesha Lane, a resident of West Palm Beach, Florida. Ms. Lane allegedly stole the identity of a co-worker by obtaining a driver's license in the victim's name. With that driver's license, Ms. Lane apparently withdrew more than $13,000 from the victim's bank account and charged approximately $4,000 on fraudulently obtained credit cards. Like Ms. Purdy who victimized a Vermonter, Ms. Lane faces charges under the "Identity Theft and Assumption Deterrence Act."
- In July, 1999, a federal grand jury in Columbus, Ohio, indicted nine individuals for Identity Theft. In this case, the thieves used 36 fake or stolen names and checking accounts to set up false bank accounts and withdraw real money. Officials in Columbus say that this case represents one of the most complex identity theft cases ever seen in the district.
- In October, 1999, Anthony Jerome Johnson, a California man, pled guilty to a federal charge of identity theft. Mr. Johnson admitted stealing the identity of Donald Lightfoot and opening two bank accounts in Lightfoot's name, as part of a scheme to obtain $764,000.

The law we passed made prosecution of these individuals, and restitution to these victims, possible.

Assisting crime victims is of critical concern to me and one I know is shared by Chairman Kyl and Senator Feinstein. The "Identity Theft and Assumption Deter-

rence Act'' provides important remedies for victims of identity fraud. Specifically, the law makes clear that these victims are entitled to restitution, including payment for any costs and attorney's fees in clearing up their credit histories and having to engage in any civil or administrative proceedings to satisfy debts, liens or other obligations resulting from a defendant's theft of their identity. In addition, the new law directs the FTC to keep track of consumer complaints of identity theft and provide information to victims of this crime on how to deal with its aftermath.

The FTC has done a good job with the statutory mandate we gave them, and I commend the Commissioners and staff for their work. The Federal Trade Commission provides user-friendly assistance to victims of identity theft on their website. The website informs victims of what they need to do right away, such as calling the fraud departments of the three major credit card bureaus. Also, the Federal Trade Commission provides an easy to fill out on-line complaint form to help the FTC track and combat identity theft, as well as links to other government agencies on this issue. Victims of identity theft can check out this site and learn about the applicable state and federal laws, learn about recent identity theft-related cases from around the country, and other helpful reports.

The ''Identity Theft and Assumption Deterrence Act'' was an important accomplishment, but there may be more we can and should do to address this problem. I look forward to reviewing the testimony of the witnesses to evaluate how well the new law is working for law enforcement and, most importantly, for the victims of identity theft crimes.

Senator KYL. In addition, we have for the record statements provided by Susan Herman, Executive Director of the National Center for Victims of Crime, which has been very, very helpful to us in putting legislation together, and also testimony of James Huse, Inspector General, Social Security Administration. Both of those statements are very helpful and will be submitted for the record.

[The prepared statements of Ms. Herman and Mr. Huse follow:]

PREPARED STATEMENT OF SUSAN HERMAN, EXECUTIVE DIRECTOR OF THE NATIONAL CENTER FOR VICTIMS OF CRIME

Chairman Kyl and members of the Subcommittee, we appreciate the opportunity to offer testimony on the important issue of identity theft and our response to victims of this pervasive crime.

The number of identity theft cases is growing. Annual case estimates are in the hundreds of thousands. Identity theft is a crime that can strike any of us, yet its victims have been marginalized, essentially left struggling to restore their good name and credit as best they can. Since identity theft offenses are relatively new, and certainly newly prominent, neither law enforcement nor victim services have yet developed an adequate response.

The National Center for Victims of Crime operates a toll-free information and referral line for victims of crime. One of the most frequent complaints we get from victims of identity theft is that law enforcement will not take a report. This is a significant problem, because victims are routinely advised to get a copy of the police report to use in clearing their credit record.

Until recently, the only official ''victim'' in many cases of identity theft was the defrauded merchant or credit agency. The individual's liability for wrongfully incurred charges was generally limited, although it could take days of persistent phone calls and letters on the part of that individual to establish that point. Today, about half of the states have defined a separate ''identity theft'' offense, under which it is clear that a person whose identity is stolen, including cases of credit card fraud, is also a victim in the eyes of the law. However, even in those states, law enforcement officers often mistakenly inform individual victims that only the financial institution or commercial entity is a ''victim.''

Victims have also been told by law enforcement that they can't take a report until they know where the crime was committed, Since identity theft can be committed in person, over the phone, through the mail, or over the Internet, this information is rarely available. Many laws state that the crime may be deemed to have occurred where the victim lives, but many front-line officers appear to be unaware of such provisions, perhaps because they have been inadequately trained.

Even where police take reports, relatively few cases of identity theft are solved. The San Diego Police Department reported that in 1999 there were 783 cases of identity theft, but only 50 ended in arrest. The Los Angeles Police Department received more than 3,000 reports of identity theft in 1999, but its Financial Crimes

Division only solved about one percent of such cases. Since cases of identity theft can be very difficult to solve, they can drive down a police department's success rate.

Victim service agencies have also not developed adequate services for identity theft victims. Currently, few resources are available. While the National Center has a referral database of thousands of agencies and organizations serving victims of crime, fewer than a dozen report that they serve victims of identity theft. And many of those simply take reports. They do not have crisis lines, nor do they provide counseling or any intervention or advocacy on behalf of identity theft victims.

Perhaps one reason there are few services for victims of identity theft is that guidelines for victim assistance grants from the Victims of Crime Act (VOCA) Fund were changed only recently to allow funds to be used for services to victims of financial crimes. With VOCA's historical emphasis on victims of violent crime, many victim service agencies remain unaware of this change and need active encouragement to develop those services.

Victims of identity theft often do not know the full extent of the crime for a long time. It can take one or more billing cycles for charges to appear on a bill. In the case of stolen checks, new instances of fraud can surface slowly over time. The person who has stolen their identity may commit crimes using that identity, giving the victim a criminal record that may resurface with any routine traffic stop or background check.

A victim's financial security can be shattered. Even if they can limit their financial losses, it can take countless hours of work over several years to repair the damage to their credit rating and to restore their good name. Credit reporting agencies can be slow to change the credit record; fraudulent charges can reappear on the victim's account or credit report after once being removed; and bill collectors can appear time and again to attempt to collect wrongfully-incurred debt.

Victims who obtain a criminal record through the misuse of their identity have a particularly difficult time clearing their names. Police records, often incurred under the victim's social security number as well as name, can be hard to change. Some states are considering legislation that would require courts, in cases of identity fraud, to make a specific finding that the person whose identity was falsely appropriated to commit the crime is innocent of the crime.

The effects of identity theft on victims are not well understood. Many victims become hypervigilant; the fraudulent misuse of their personal information makes them keenly aware of how many people in their daily lives have access to their credit card information or social security number. They find themselves unable to trust the billing staff at their doctor's office, the department store clerk, their office administrator, or the secretary at their child's school. This inability to trust others in the ordinary business of life. takes an emotional toll on victims.

Victims of identity theft also are excluded from many state level victims' bills of rights. Victims who have had their identity misappropriated often have a great interest in being kept apprised of the-progress of the case, yet they have no legal rights to be kept informed or to participate because those rights are limited to victims of violent offenses.

The federal Identity Theft and Deterrence Act of 1998 and many new laws at the state level have made significant improvements in our nation's response to victims of identity theft. However, as this problem continues to grow, it is clear there is more that we can and should do. Every victim of crime deserves adequate resources and assistance to rebuild their lives, even victims of non-violent crime such as identity theft. The incidence of identity theft is growing, and it is time to strengthen our national response.

PREPARED STATEMENT OF JAMES G. HUSE, JR., INSPECTOR GENERAL, SOCIAL SECURITY ADMINISTRATION

It is an honor to provide this Subcommittee with the Social Security Administration's Office of the Inspector General's (SSA–OIG) status of ongoing work and our perspective on the direction we need to take to reduce the incidents of identity theft. Thanks to the leadership of Senator Kyl and the efforts of this Subcommittee, the Identity Theft and Assumption Deterrence Act of 1998 (Identity Theft Act) was passed in October 1998. That Act provided this office with a powerful weapon to combat Social Security number (SSN) misuse when used to commit identity theft. While the SSN was never intended to be a "national identifier," this Act acknowledges that the SSN is a commonly used means of identification. Even before the passage of the Identity Theft Act, this office had gained insight into the widespread occurrence of identity theft, because of the vast number of complaints received by the SSA–OIG Fraud Hotline. Because of this, we developed an action plan to focus

on SSN misuse. The American public has an expectation that the Government will establish safeguards to protect their SSN's from misuse. They also expect governmental action when misuse occurs. This office will do its best to meet the public's expectation.

From the beginning, our office has taken a proactive stance to work with other Federal organizations to reduce the incidents and impact of identity theft crimes by participating in national and international work groups. We worked closely with the Federal Trade Commission (FTC) to develop informational materials that provide a consistent message throughout the Federal Government to assist and educate victims of identity theft. We have met with several U.S. Attorney's Offices to discuss the prosecutorial guidelines for identity theft and because this issue is so important, I have detailed an attorney from my office to the Department of Justice to assist in the prosecution of identity theft cases.

Our office continues to share knowledge and data with the FTC. The FTC and our Office of Investigations are developing a referral system that will allow for the automated transfer of data between the agencies. This referral system will not only improve our ability to assist victims but allow us to detect individuals committing identity theft more quickly. Based on a recent analysis by FTC, we estimate that referrals of SSN misuse could reach 8,000 a month in addition to the 2,500 we already receive. Because of this expectation, we are redesigning our systems to capture SSN misuse referrals in a more defined structure that will delineate SSN misuse by type.

Our Office of Investigations is using existing programs to further develop the referral process with the FTC. The fugitive felon program—designed to implement sections of the Personal Responsibility and Work Opportunity Reconciliation Act of 1996 (commonly known as the Welfare Reform Act)—identifies individuals illegally receiving Supplemental Security Income (SSI) payments through computer matching agreements with State and local law enforcement entities. Oftentimes, these data matches identify individuals whose SSN has been assumed by a fugitive. We refer this information to the FTC and our investigative units follow up on leads of those individuals who assumed the victim's SSN.

In fiscal year 1999, our Office of Investigations launched SSN misuse pilot projects in five cities across the Nation. Our special agents provide the lead in working with Federal and State law enforcement agencies to review Hotline allegations and open an investigation, if warranted. Partnering with other law enforcement agencies allows us to have a greater impact with limited resources. Because of this partnership, we are able to present cases for prosecution, which if presented separately, would not be accepted. In the past year through these task forces, we opened 79 investigations, which so far, have resulted in the conviction of 18 individuals. U.S. Attorney's Offices and Federal and State law enforcement agencies have enthusiastically welcomed these pilots and have applauded my office for taking the investigative lead. In one city, Federal and State law enforcement agencies that were not part of the task force have asked to join because of its success.

I would like to provide the Subcommittee with a synopsis of three different investigations related to SSA programs and identity theft that were successfully prosecuted.

In the first case, our Office of Investigations was instrumental in the conviction of what is believed to be the first Federal prosecution under the Identity Theft Act. Our Milwaukee Sub-office opened an investigation, based on a referral from the Wisconsin Capitol Police, of Waverly Burns who was receiving SSI payments. During the course of the investigation, we discovered that Mr. Burns acquired the SSN of another individual and then used this number to secure employment as a cleaning crew supervisor. While working in this capacity, he gained access to the offices of the Wisconsin Supreme Court and stole over $80,000 in computer equipment. Meanwhile, he lied to SSA officials, in a statement for determining continuing eligibility for SSI, claiming that he was unemployed and continued to receive full SSI payments. Mr. Burns used the stolen SSN to secure a State of Wisconsin identity card, to open bank accounts and file fraudulent tax forms under the victim's name and SSN.

On April 21, 1999, Waverly Burns was indicted for identity theft, SSN misuse, and making false statements to SSA and the Internal Revenue Service. On May 5, 1999, OIG Special Agents arrested Mr. Burns after tracking him to Chicago. Mr. Burns pled guilty to using the identity of another person to obtain employment, then using that employment to commit burglary. Mr. Burns was sentenced to 21 months in prison and ordered to pay over $62,000 in restitution directly to the Wisconsin Supreme Court.

In the second case, our SSA/OIG special agents as part of the Delaware Financial Crimes task force, investigated Zaid Gbolahan Jinadu as he schemed to defraud sev-

eral federally insured financial institutions. He solicited the assistance of bank employees to provide SSN's and other identifying data to open fraudulent credit card and bank accounts. These compromised employees also helped him to take over current accounts, make fraudulent wire transfers, receive cash advances and negotiate numerous checks. Mr. Jinadu was indicted by a Federal Grand Jury in the District of Delaware on October 26, 1999, on four counts-one count each of bank fraud; identity theft; fraud in connection with access devices; and misuse of SSN's. On December 20, 1999, Mr. Jinadu and his co-defendants entered a guilty plea to one count of bank fraud and one count of identity theft. He is responsible for fraud losses of approximately $281,122. Total known losses to financial institutes by Mr. Jinadu and his cohorts during the past 4 years exceeds $4 million.

In our last case and perhaps one of the most egregious of identity theft crimes was one perpetrated against an elderly individual. Our Richmond Sub-office opened an investigation on Charles Fleming, a SSA disability beneficiary, who stole the identity of a 67-year old individual recovering from a stroke. He took personal documents from the victim's home and used them to obtain a State driver's license and SSN under the victim's name. Using these documents, he opened credit card and loan accounts and found work. He concealed this employment from SSA in order to continue receiving full disability benefits. Mr. Fleming pled guilty to identity theft and received a sentence of 12 months and 1 day in a Federal penitentiary and 3 years of supervised release. The court ordered him to pay restitution to SSA of over $29,000 and to creditors of over $24,000. The victim is in the process of repairing his credit rating with the assistance of FTC.

While it is apparent that our initial action plan has been successful, we have recognized that identity theft is on the increase and we need to expand our role. I believe the SSA–OIG should continue to lead the law enforcement community in the investigations of SSN misuse and identity theft to ensure the integrity of the SSN and SSA's programs. Because of this, I directed our Offices of Audit and Investigations to work together to define the most susceptible areas where SSN misuse and identity theft impact on SSA's programs. After completing this analysis, I focused our investigative resources on the following areas involving SSN misuse if:

(1) there appears to be a failure of SSA's enumeration business process or the wage and earnings reporting system, since discrepancies in this vein can be indicative of SSN misuse;

(2) there is the suspicion or an allegation involving the counterfeiting of SSN's;

(3) there is concealment of work activity by false identification, especially to obtain or maintain eligibility for SSA benefits; and/or

(4) there appears that a fake SSN is being used to maintain a fictitious identity for the purpose of receiving other Federal and State program benefit payments.

The Office of Audit has also been instrumental in providing recommendations to the Agency that, when implemented, will strengthen the integrity and security of the enumeration function. Enumeration is the process by which SSA assigns original SSN's, issues replacement cards to individuals with existing SSN's, and verifies SSN's for employers and other Federal agencies. SSA issues about 16 million new and replacement cards annually. There are nearly 300 million active cards at this time.

Over the past 3 years, members of Congress have asked the Inspector General community to identify the most significant management issues facing their agencies. In my most recent response I included identity theft. False identities are being used to defraud SSA.

Unscrupulous individuals can assume the identity of another person who is either alive or dead and work under the stolen identity. Individuals have also assumed the identity of another person and placed their assets under this identity in order to qualify for SSI payments under their own SSN. I have shared this assessment with the Agency and recommended that they concentrate on the prevention rather than the detection of identity fraud. Because of this, I am also encouraging the Agency to include SSN fraud and misuse as a key initiative in their Strategic Plan.

In addition, SSA's Deputy Commissioner for Finance, Assessment and Management and myself are co-chairs of the National Anti-Fraud Committee. We formed this Committee to facilitate an exchange of ideas—determining what problems we face and suggesting solutions. The Committee is comprised of 10 Regional Anti-Fraud Committees located throughout the country. In the past year, identity theft and SSN misuse has become a major focus for discussion and because of its importance, we have included it as an agenda item for the National Anti-Fraud Conference that will take place in September.

Currently, there is proposed legislation before the Congress asking to extend civil monetary penalties to those committing crimes involving the misuse of a SSN, who are not being punished by the Federal courts. I urge you to endorse this legislation. There are other legislative remedies such as statutory law enforcement that will enable our investigative offices to process these cases more efficiently and I hope that you support this as well.

I thank the Subcommittee for giving me this opportunity to inform you of our work in the identity theft arena. I pledge, with your support, to vigorously attack the problem of SSN misuse and identity theft before it becomes a national crisis. I would be more than happy to provide the Subcommittee with any additional information or to answer any questions that may arise from these Hearings.

Senator KYL. In addition, we will keep the record open for either questions or statements of Senators who could not be here. And as I say that, Senator Grassley also has arrived. So, Senator Grassley, thank you for being here.

Let me read a brief opening statement and then I will call upon Senator Grassley and then hear from our first witness.

One of my goals as chairman of this subcommittee has been to prevent criminals from using technology to prey on society. There are few clearer violations of personal privacy than actually having your identity stolen and then used to commit a crime. Criminals often use Social Security numbers and other personal information of law-abiding citizens to assume their identity and steal their money. It is high-tech theft.

To combat this, I sponsored the Identity Theft and Assumption Deterrence Act, which is now Public Law 105–318, which prohibits the stealing of a person's identity. The aim of the Act is to protect consumers and safeguard people's privacy. The bill was prompted by Bob Hartle, of Phoenix, who approached me about the problems he had suffered at the hands of an identity thief.

With overwhelming bipartisan support, the bill became law in October of 1998. Under the law, a conviction for identity theft carries a maximum penalty of 15 years' imprisonment, a fine, and forfeiture of any personal property used or intended to be used to commit the crime. The bill also provides that the Federal Trade Commission must assist people whose identities have been stolen.

Violations of the Act are investigated by Federal law enforcement agencies, including the U.S. Secret Service, the FBI, the Postal Service, and the Social Security Administration Office of Inspector General. Federal identity theft cases are prosecuted by the U.S. Department of Justice.

Under the law, the Federal Trade Commission collects complaints about identity theft from consumers who have been victimized. The Commission helps victims of identity theft by providing information to assist them in resolving the financial and other problems that can result from this crime.

It has now been 16 months since the law was signed by the President. The Office of Inspector General of the Social Security Administration released a report in August of last year, 10 months after the bill was signed into law. According to this report, 81.5 percent of Social Security number misuse allegations relate to identity theft.

The report reaches the following conclusion: identity theft affects many areas of our society. Private citizens have had their credit histories destroyed by individuals who steal and use their Social Security numbers to obtain credit. These individuals run up large

credit debts and then move on without paying the debt. This type of behavior not only destroys the citizen's credit history, it adversely affects the national economy as creditors raise interest rates to cover the losses arising from this fraudulent activity. Identity theft can, therefore, as the report shows, have a devastating effect.

One purpose of this hearing today is to survey the effect of Public Law 105–318. The new law, I would say, seems to be working quite well. For example, in February the law was used to charge two men suspected of being involved in terrorist activities targeting the United States.

Additionally, according to statistics from the Department of Justice for fiscal year 1999, 1,147 cases were opened, involving 1,350 possible defendants, including 169 cases opened in the District of Arizona, my State, involving 178 possible defendants. Five hundred thirty-five cases were closed, with 644 defendants being sentenced nationwide. Ten cases were closed in Arizona, with 13 defendants being sentenced. Of the 644 defendants sentenced, 407 entered guilty pleas. In Arizona, of the 13 defendants sentenced, 10 entered guilty pleas.

Today, the subcommittee will hear from three witnesses about the effect of the Identity Theft and Assumption Deterrence Act. Maureen Mitchell, from Madison, Ohio, is a victim of identity theft and will discuss her case for us.

Gregory Regan is Special Agent in Charge of the Financial Crimes Division for the Secret Service, which is one of the primary Federal law enforcement agencies investigating identity theft.

Finally, the subcommittee will hear from Jodie Bernstein, the Director of the Bureau of Consumer Protection of the Federal Trade Commission. She will discuss how the FTC has responded to identity theft in carrying out its duties under the 1998 law.

In closing, I would like to thank Senator Feinstein for her support in helping the identity theft bill to become law. As always, I must say it is a pleasure to work with her on subcommittee initiatives that aim to ensure that the law keeps pace with technology. I also give my thanks to Senator Grassley and other members of the committee who have worked very closely with me in pursuing these particular kinds of issues.

Before we hear from Ms. Mitchell, let me ask Senator Grassley if he would like to make an opening statement.

STATEMENT OF HON. CHARLES E. GRASSLEY, A U.S. SENATOR FROM THE STATE OF IOWA

Senator GRASSLEY. Thank you very much for holding this hearing, following up on the effectiveness of the identity theft law that you were so instrumental in getting passed within the last couple of years. I think the hearing shows a recognition of the fact that it has become a very serious problem and we may need to do more about it.

I think you have adequately described what the problem is. I am here today to make sure that the laws adequately protect the victims and that the criminals get the punishment they deserve. If there are any changes that need to be made to make this law better, I am ready to work with you on doing that.

I am very concerned about how the Internet can facilitate this crime. While a lot of this information has been available through other sources for a long time, the Internet and other interactive computer services make collecting personal information extremely simple. It is kind of like one-stop shopping.

Through government and corporate resources readily available on the Internet, an identity thief or stalker can collect information necessary to find his or her victim. This poses a real threat to all of us, but especially I am concerned—and this comes from my work as chairman of the Aging Committee—about the impact upon the elderly. So while the Internet has brought about incredible changes for the better, the legal system needs to be there to adequately safeguard the confidentiality of individuals' personal records.

I am also concerned about the fact that personal information is being marketed without the knowledge of the persons affected. I have expressed my concern on a number of occasions about cookies and other devices that collect information about unsuspecting individuals using Web sites. And I have been particularly concerned about the ease with which a person's Social Security number can be utilized in stealing identity.

In the last Congress, Senator Feinstein and I introduced legislation to prohibit the commercial use of Social Security numbers and to restrict their use by State departments of motor vehicles, especially for commercial use. This bill would have gone to the source to stop the dissemination of Social Security numbers which criminals use all to easily to steal people's identities. Unfortunately, we are now playing catch-up because technology advances so rapidly. But this is such a problem, I want to reintroduce this legislation to protect our constituents.

Chairman Kyl, I hope that we can explore these difficult policy issues here in this subcommittee through this hearing and other meetings, and I want to work with you on any necessary changes or enhancements of the identity theft law. This is not a victimless crime and it should not be treated as such.

Senator KYL. Thank you very much, Senator Grassley, and you are absolutely right. We are taking a survey of the situation today to see whether there are changes that need to be made, to see how well the law is working. And as you also pointed out, as technology evolves, we are going to have to constantly keep tracking it and keep up to date because it can obviate the work that we do in this committee pretty fast if we don't continue to monitor it.

Well, our first witness today is an actual victim of identity theft, and I thought it would be interesting to have you basically hear her case, her situation, to see how this crime can occur, how devastating it can be, and what can be done about it.

Ms. Maureen Mitchell is a registered nurse and a licensed realtor. She lives in Madison, OH, with her husband, Raymond Mitchell. They have two children. She and her husband are victims of identity theft resulting in fraud in excess of $110,000.

Ms. Mitchell, it is a pleasure to have you with us here today.

STATEMENT OF MAUREEN MITCHELL, REGISTERED NURSE AND LICENSED REALTOR, MADISON, OH

Ms. MITCHELL. Thank you, Senator Kyl. It is a pleasure to be here.

My husband and I have been married for 23 years. We have always been financially prudent and fiscally responsible people. We have never paid a debt late in our lives. We use credit conservatively and wisely. We have a daughter in college and a son in high school. We have always taken the normal consumer protections to try and keep our private information private. We do not throw out pre-approved solicitations intact, we do not bank on the Internet, we don't order via the Internet. We don't order merchandise through home shopping networks. When we do use our credit card, we are conscientious and always obtain a receipt.

In spite of all these precautions, we found ourselves getting a phone call from our KeyBank Mastercard service provider in September alerting us to an unusual pattern of activity on our credit report that, based on our consumer profile, caused them some concern.

It turns out there were a few thousand dollars' worth of mail order charges placed on our Mastercard. We had never lost our wallets, we never lost our credit cards, we had never been burglarized. Yet, our account number was compromised. KeyBank notified us. They closed our account. They reported the card lost or stolen, which we objected to because that is not what happened. They issued us new credit cards, and we thought that would be the end of it.

We asked if there was anything else that we needed to do and we were told no. I asked about making out a police report and I was told that it was optional. I did make out a police report on September 12 and reported the fraudulent use of our credit card number. Two months later, on November 15, we received a phone call from J.C. Penney informing us that someone had used my husband's name and Social Security number to open an account at a Penney's store in Schaumburg, IL. We reside in Ohio.

Penney's suggested that we call and place consumer alerts and fraud alerts on our credit reports with Trans Union, Experian and Equifax, which we did, and Penney's kindly provided us with those phone numbers. When I called Trans Union, I was dismayed to learn that there had been 25 inquiries into our credit in a 60-day period. There hadn't been 25 inquiries into our credit in the entire 23 years that we had been married, and I asked Trans Union did that not send up red flags to them. The response I got was that it was not their job to monitor the number of inquiries. They did kindly give me the names and phone numbers of those 25 merchants.

I then called Experian and found out that there had been six changes of address filed in that 2-month period of time. We have resided at the same residence for 20 years. Yet, six addresses now appeared on our Experian credit report. I spent the next few days frantically trying to call the merchants who had made inquiries into our credit report to alert them that we were not the applicants and to beg them not to extend credit in our name.

I encountered automated answering system hell in trying to notify these merchants. I was never offered the option of pretending I had a rotary phone to speak to a human being, was never offered the option of pressing an extension to report fraud, was frequently asked to enter an account number, and I didn't have an account number because we are not the ones who opened the account. It was an effort in frustration and futility, but I did persist.

Three days after we placed fraud alerts on our consumer credit reports, we received three very alarming phone calls in a 2-hour period of time. One was from Citibank, one was from BankOne, and one was from Marquette Bank. Forty-five thousand dollars of fraudulent loan applications had been made in a 2-hour period at three different lenders in close geographic proximity to each other in the greater Chicago area using my husband's name and Social Security number.

BankOne faxed us an affidavit. We signed it, we had it witnessed, we faxed it back. The Lansing, IL, detectives apprehended a suspect as he left BankOne with the $15,000 he had obtained fraudulently. This suspect was found to have an Illinois driver's license and an Illinois State identification card with his own picture on it, but my husband's name, my husband's Social Security number, my husband's vital statistics. This suspect said to the detectives as he was arrested, I did not use a gun, I did not use a knife, call my lawyer, I will plead guilty and they will put me on probation.

The detectives ran the suspect's fingerprints and he was found to have 17 aliases and multiple priors. Yet, 2 days later, Judge Thomas Panicki, in Cook County, IL, released this suspect on his own recognizance on a signature bond. We were appalled. These criminals know that if they use a weapon to commit bank robbery, they will do mandatory jail time. Technology has now become their weapon, but it is not the typical gun and knife, and they are counting on being put on probation instead of incarceration.

When this criminal was apprehended, it was only the tip of the iceberg of the information of the damages that were done fraudulently that was available. We have subsequently learned that a Lincoln Navigator was purchased using our credit. A Ford Expedition was purchased using our credit. Service Merchandise accounts were set up. Household bank accounts were set up. They are living large using our names and credit.

The scales of justice here seem to be tipped in the wrong direction. This criminal is assumed innocent until proven guilty. Yet, the victim of identity theft is assumed guilty until proven innocent. We have had to prove our innocence over and over again to 30 different merchants, 30 different ways. This criminal is given a public defender to protect his legal rights. Yet, if we need to hire an attorney to clean up this mess and protect our rights, we are paying substantial legal fees out-of-pocket.

It has come to light subsequently that the person who purchased the Ford Expedition is not the same person who was apprehended as he left the bank. This is an identity theft ring that is operating in an insidious manner. The detectives who apprehended this suspect are limited by their geographic boundaries to the community in which they work for their investigation. Yet, similar crimes are

being committed in surrounding communities, but the detectives are limited; they can't investigate those crimes.

We have begged, pleaded, cajoled. We have submitted notarized statements. We have over 100 pages of documentation on this. I have met with our Congressman, Steve LaTourette. He put me in touch with the FBI. I have met with the FBI. It was only through the intervention of Senator Kyl's office that we were actually able to obtain the Secret Service as the investigative authority in this case.

As victims, we have found it to be a nightmare on filing out the forms and affidavits that are required by the individual merchants to prove our innocence. I strongly urge that there be a uniform protocol established for victims to fill out one set of forms and one set of documents.

We were very fortunate early on in making our phone calls that I had contacted the Ohio Attorney General's office and they steered us to contact the Federal Trade Commission. The Federal Trade Commission advised us that we needed to contact the Social Security Administration, the Department of Motor Vehicles, the Internal Revenue Service, possibly our employers, and all of the other avenues where your Social Security number is your identifying number. Kathleen Lund, of the Federal Trade Commission, provided us with good information, and also moral support at a very difficult time.

It is almost indescribable to try and put into words what it feels like to be a victim of identity theft. It has a huge impact. We were told by the detectives in Illinois that we needed to keep fraud alerts on for the rest of our lives because the criminals know when the fraud alerts expire and our information will be recirculated again. So the next time my husband and I go to apply for a loan, whether it be for a vehicle or to put our other child through college, we will have to explain this story to the merchant, hope they believe us, and hope that they don't perceive us to be the criminals.

Prior to the Identity Theft Act going into effect, we wouldn't have even had a legal standing as victims here. We wouldn't have been considered true victims. We are indeed victims, but we are all victims because we are all paying for this in the higher cost of consumer goods and the higher cost of interest rates. The attempts on our credit exceeded $150,000. The actual amounts obtained are $111,00, and they may still be climbing. There may be information that we do not know as of yet.

The criminals need to be held accountable. Technology needs to be considered as a weapon, as serious a weapon as a gun or a knife. We were thrown into a financial quagmire through no carelessness on our part. We don't know how they obtained our information, and all of us are vulnerable. People need to know that the Federal Trade Commission is the national clearinghouse on identity theft. They need to know that they are entitled to Federal investigation for these crimes, and that as victims we have rights to try and protect ourselves and assist in the prosecution of criminals.

I included in my statement a list of 15 recommendations for your review. I thank you for your time. I appreciate this opportunity, and I hope you all never walk in the shoes of an identity theft victim.

Senator KYL. Thank you very much, Ms. Mitchell. I think that brings alive the nature of the problem that is faced here and makes it clear why we have to ensure that our law works.

One of the things you did was to provide 15 specific recommendations for us. Let me begin by asking what more you think the FTC could or should be doing in a situation like this. In other words, did our attempt to provide a clearinghouse activity with the FTC work? Could it work better? What would you recommend in that regard?

Ms. MITCHELL. I found that the information that we received from the FTC was very valuable and very important for us. There were things that we would not have thought of, bureaus to notify, the Social Security Administration, the Internal Revenue Service. We were so focused on trying to notify the merchants to prevent further financial damage that we may have indeed overlooked those other things.

I strongly urge that there be a uniform protocol for victims, one set of documents once it is established that you truly are a victim of identity theft. We have had to submit handwriting samples to 20 different merchants. We have had to submit notarized statements and affidavits. It is like filling out your income tax returns 20 different times with 20 different sets of instructions. A uniform protocol for victims to follow, I think, would make—it is not easy to walk in these shoes. Whatever we can do to make it easier would be appreciated.

Senator KYL. That is an excellent suggestion and we will pursue that with our later witnesses.

You also note that the police departments and local law enforcement agencies need to know more about the Federal law so that they will understand how it works and how they can take advantage of it. I think that is a good idea and we are going to have to try to figure out some ways to make sure that that information gets out.

Is there anything else, one of the specific recommendations that you would like to bring not only to our attention but to the attention of the public at large here?

Ms. MITCHELL. I think the credit reporting agencies and the merchants who were defrauded of merchandise have an onus of responsibility here. KeyBank alerted us to an unusual pattern of activity on our credit report based on a consumer profile that has been developed about us for the last 20 years that we have been their customers. Trans Union, Experian and Equifax also have consumer profiles about us for our entire adult lives.

We hadn't moved in 20 years. Why would they assume that moving 6 times in 2 months was not something to be alarmed about? We had never over-extended ourselves with credit. Yet, there were 25 inquiries in 2 months that didn't send up red flags to them. I think they are the first line of defense.

It is already too late to safeguard the Social Security numbers; they are out there. We live in a State where our Social Security number up until recently appeared on our driver's license through no choice of ours. We had to have it that way. I think the credit reporting agencies can be a good first line of defense for the consumers. We did take precautions ourselves and they were not

enough, and the credit reporting agencies are the ones—the accuracy of the information on your credit reports is very important. The merchants use that and perceive it as gospel because it came from the credit reporting agency. Yet, there doesn't seem to be a system of verification of that information prior to it being entered on your credit report. That needs to be remedied.

And I also can tell you that in the example of them buying a Ford Expedition, there were four glaringly obvious errors on that application. Our name was misspelled. There were two co-buyers who said they resided together. Yet, one used an address of North Grand and one used an address of West Grand on this application. They purchased the 60,000-mile extended warranty at the cost of $695. When that figure was transposed over to the debit column, it was transposed over as $1,695. I don't know how the merchants and lenders missed this.

They also put down the area code to verify their place of employment as 300. That area code does not exist in the continental United States. Yet, this loan was approved, and it was a $40,000 vehicle. The credit reporting agencies need to use due diligence and the merchants need to use due diligence.

Senator KYL. Thank you.

Senator Grassley.

Senator GRASSLEY. I have three short questions. After all you have been through—and by the way, I have a staff person whose sister and parents were victims, whether to the extent you were, I don't know, but they were victims of stolen identity.

After all is said and done, did you ever find out how the criminals got your information?

Ms. MITCHELL. No, we haven't. Unfortunately, Senator, we are not all said and done yet. The case has not come to trial. We do not know how they obtained our identity. We do not believe it was through any carelessness on our part. And we would like to know how it was accomplished, but right now we do not know.

Senator GRASSLEY. Is this something that the police can't tell you or won't tell you? Is it some big secret?

Ms. MITCHELL. I don't believe the police departments know at this point how these people got this information about us. We reside in one State; the criminals and the criminal activity is taking place in another State.

Senator GRASSLEY. Now, you spoke about a central location you ought to be able to go to and have one form or one way of filling out a document indicating that you have been defrauded and to get the information out. I am aware of some companies that provide a centralized service where consumers can register their credit cards and make only one call if the cards are lost or stolen.

Do you happen to know if these companies provide any assistance with regard to identity fraud?

Ms. MITCHELL. I don't know that, Senator. I know I encountered numerous merchants with numerous automated answering systems that never offered us the option of reporting fraud by pressing a button. I don't know about the consumer credit card companies. We only had one credit card number compromised. The remainder of what happened to us is that the criminals assumed our identity. It is not that they accessed our accounts. They posed as us.

Senator GRASSLEY. Will the credit bureaus include the fact that your identity was stolen on the face of the credit report, as well as reference police reports and the FTC reference number?

Ms. MITCHELL. I am glad you brought that up, Senator. Since we have placed the fraud alerts on our credit reports, we have received updated credit reports periodically, almost monthly. The fraud alerts on our consumer credit reports appear on the back page of the credit report, in the same size type as the rest of the information.

In my recommendations, I put down that I strongly believe that the fraud alert should appear on the front page of the credit report, in bold-face type, to reduce the possibility of it being overlooked. Consumer credit reports can contain eight, nine pages of information of a 25-year credit history. Putting the fraud alerts on the last page maximizes the opportunity of it being overlooked. Placing it in bold-face print on the front page minimizes it from being overlooked.

Senator GRASSLEY. So in other words, it is helpful, but it could be a lot more helpful?

Ms. MITCHELL. Yes, it can.

Senator GRASSLEY. Thank you, Mr. Chairman. Thank you.

Ms. MITCHELL. Thank you, Senator.

Senator KYL. We are talking about your recommendations up here.

Ms. MITCHELL. OK.

Senator KYL. So I think having you present not only the story of what happened to you and how, but also the kinds of problems you have encountered and your specific recommendations on how to deal with it has been very, very helpful. I would like to thank you especially for that, as well as taking the time to come here today and to be with us to present this testimony.

We will take your testimony very seriously, and especially your recommendations, and I think it would be good if we could remain in touch with you and find out what happens not only to your case, but also to track how long it takes finally for you to be free of this problem, because it undoubtedly will suggest other things that we can do so that at least people who come later aren't going to be troubled to the same extent that you and your husband have been.

Ms. MITCHELL. Receiving the phone calls from the collection specialists was heart-breaking at first. Now, it is almost becoming somewhat of a challenge because as they call us and ask us why we have failed to make the payment for our Lincoln Navigator, we tell them the story that we didn't buy the Lincoln Navigator. And then I always end my conversation with them—I cite the Federal Trade Commission's reference number and the police department's, et cetera. I now am able to tell them through your office, appreciatively, that the Secret Service has now taken this case.

And I close my remarks with the collection specialists by saying it is ironic that you can now find the real Mr. and Mrs. Mitchell when you want your money; too bad you didn't find the real Mr. and Mrs. Mitchell before you loaned out the money.

Senator KYL. Good point, good point.

Senator Grassley, anything further?

Senator GRASSLEY. No.

Senator KYL. I really appreciate your testimony today. This has been very, very helpful, and we will stay in touch with you. Thank you.

Ms. MITCHELL. Thank you, Senator.

[The prepared statement of Ms. Mitchell follows:]

PREPARED STATEMENT OF MAUREEN MITCHELL

Mr. Chairman, Members of the Committee, my name is Maureen Mitchell and it is a privilege to have been invited to submit this testimony today.

I am 44 years old, my husband and I have been married for 23 years, we have a daughter in college and a son in high school. I am a Registered Nurse, and I have been a licensed Realtor for 20 years.

My husband and I have always been financially prudent and fiscally responsible people. We have never overextended ourselves, and we have always paid our bills in a timely manner. We also have exercised the normal consumer precautions to ensure our privileged information remains private. We have never lost our wallets, never been burglarized, we obtain the receipts when we make credit card purchases, we don't bank on the Internet, we don't order merchandise via the Internet, we don't order through home shopping networks, we rarely order from catalogs, and we always tear up the pre-approved solicitations that arrive in the mail prior to disposing of them to prevent someone from "dumpster diving" and obtaining our information. We have never given our personal account numbers or social security numbers over the phone. We even checked our credit reports in March of 1999 to ensure their accuracy. In spite of all the precautions we have taken, we are now victims of identity theft.

It started on a Sunday afternoon, September 12, 1999, when we received a phone call from our KeyBank Mastercard Service Center questioning an unusual pattern of activity on our credit card. After much discussion with the Service Center representative, it was verified that neither my husband nor I had authorized or made the charges to the account. I was told our credit card would be canceled, it would be reported lost or stolen, and new cards would be issued. I objected to the cards being reported lost or stolen because they were not: my husband had his card in his wallet and I had mine in my wallet. Nonetheless, I was told the cards had to be reported lost or stolen to close the account (I subsequently learned that we could have insisted that the account be closed at the request of the consumer due to fraudulent use).

I was also told by the Service Center Representative to contact KeyBank Special Services when they opened for business on Monday morning. I called KeyBank Special Services at 8:15 A.M. Monday morning and was told that four attempts were made to place charges on our account, three were approved and the fourth was declined because the bank became suspicious due to the unusual level of activity on our credit card. KeyBank was able to determine the charges were made via a phone order, not by someone actually having our credit card. The amount obtained fraudulently was $2,164.55. I then went to our local KeyBank, branch office (where we've banked for twenty years) to inform them about the phone call from the Service Center, to verify the account was closed and to inquire if there was anything else I needed to do. I was told that there was nothing else I needed to do: the merchant slips would take a week to come into the bank, and the bank would look into it. I asked if I should make out a police report and was told that it was an option but not really necessary. The bank would issue us new credit cards with a different account number, the fraudulent charges would never appear on our billing statement, and our new cards would arrive in two weeks. I did, however, file a police report with our local police department to report the fraudulent use of our KeyBank Mastercard number. If KeyBank would have advised us, at this point, to place Fraud Alerts on our credit reports, the following events would not have occurred.

On November 15, 1999 we received a phone call from J.C. Penney's credit department advising us that an account had been opened in Illinois using my husband's name and social security number. A line of credit had been extended in my husband's name, the persons making the application said they were our niece and nephew and were authorized users. When J.C. Penney's sent the bill to the address given on the application, it was returned by the post office because "no such house number existed." The returned billing statement was what prompted J.C. Penney's to call us. We were advised by J.C. Penney's to immediately contact the three major credit reporting bureaus to place fraud alerts on our credit reports, and Penney's kindly gave me the phone numbers to contact. Upon contacting Trans Union, Experian and Equifax, we discovered that we had been plunged into Identity Theft Hell!

In speaking to Trans Union, I discovered there had been 25 inquiries into our credit report in the previous 60 days (from September 16 through November 15). None of those inquiries were initiated by us legitimately seeking credit. I told the representative at Trans Union that there had not been that many inquiries in the previous twenty years, and questioned whether that many inquiries in such a short time sent up "red flags" to Trans Union. The reply I received was that it was not their job to monitor the number of inquiries, and it was suggested that I call all the merchants who made the inquiries to alert them. Trans Union did provide me with the names and phone numbers of the merchants to contact. The list was extensive and included numerous car dealerships, banks, credit card companies, furniture stores, department stores, and communication service providers. Trans Union did place Fraud Alerts on our credit reports at this time.

I also called Experian and Equifax to place Fraud Alerts on our credit reports, and learned that they too showed numerous inquiries into our credit during the same 60 day period. I requested that each credit reporting agency send me a copy of our credit reports, and I spent the next three days frantically making phone calls to the merchants who had made inquiries.

I now entered automated answering system hell! As I called each merchant using the numbers provided by the credit reporting bureaus, I would be connected to an automated answering system, "Press one for English, press two for Spanish, press three to increase your credit limit, press four to check your account balance, press five to see when the last payment was posted to your account, press 6 * * *" I rarely encountered an option to speak to a human being. I never was given the option of pressing a number to report fraud, but I universally encountered the request to enter an account number (keep in mind I didn't have an account number because we were not the ones who opened the account); nonetheless I persisted through automation hell, never giving up hope that a "live person" would eventually come on the line. As the automated system requested I enter an account number, I waited; as the request was repeated, I waited; when I was unable to enter an account number instead of being transferred to a human being, I was disconnected! I then called back, went through additional automated answering system hell, and when I heard enter your account number I randomly entered 01010101010101 * * * hoping that I would eventually enter the required number of digits to speak to a human being. Instead a recording came on saying "the numbers entered do not match an account of record, please re-enter your account number." I re-entered the numbers only to find that I was disconnected again because "the account numbers do not match our accounts of record." I endured this frustration while trying to reach numerous merchants to alert them that a fraudulent application had been made using our name. This frustration of automation needs to be remedied. I strongly suggest that merchants be required to provide an option on their automated system to press a number to report fraud, and that the victim can speak to a human being!

I also contacted our local police department who sent an officer over to take our statement and file a police report. The officer instructed me to fill out the police report as accurately and as thoroughly possible. I also contacted the Federal Trade Commission's Identity Theft Hotline and spoke to Kathleen Lund (877–438–4338). Kathleen confirmed that we were indeed victims of identity theft based on the facts that I gave her. She informed me of Title 18 (Identity Theft and Deterrence Act), and told me that Identity Theft was a Federal Offense. Kathleen told me to continue to write the police report I was working on and to continue to try to call the merchants who made inquiries. She assigned a reference number to our case and gave me the phone number for the Federal Information Center (800–688–9889) to contact to see if they had merchant numbers other than the ones I had to try to circumvent the automated answering system hell I was encountering. It truly was a relief to speak to a live human being who was able to provide some guidance and encouragement during this very stressful time. Kathleen advised me to call the Social Security Administration, the Internal Revenue Service, the Department of Motor Vehicles in our home state and in Illinois, and the State's Attorney General's Office in our home state and in Illinois, to report that someone was using our credit and my husband's social security number fraudulently. Kathleen also asked me to keep her informed of any further fraudulent activity. I called the Federal Information Center and obtained the phone numbers I needed and then I made the necessary phone calls. I then continued on my mission of calling the merchants to alert them that the applications were made fraudulently.

While I was again enduring the frustration of automation, I received three very alarming phone calls. The date was now November 18 (three days after we placed the fraud alerts on our credit reports), and the first call was from Citibank in Illinois alerting us that an application for a twenty-five thousand dollar ($25,000.00) loan had just been made using my husband's name and social security number. The

application had been made in person by an individual posing as my husband. The loan officer informed me that all of the pertinent information had been verified, legitimate looking identification had been presented and everything seemed fine until the Fraud Alerts on our credit report were activated. I explained to the fraud department at Citibank that we had placed the fraud alerts three days prior, when we became aware we were victims of Identity Theft. Citibank's Fraud Department said they were going to contact their Security Department, check to see if the suspect was on their security camera and get back to me.

While waiting to hear back from Citibank, I received another phone call. It was a fraud investigator from Bank One (Thomas Retkowski) informing me that an application for a fifteen thousand dollar loan ($15,000.00) had just been made in Illinois. I informed Thomas of the prior call from Citibank, and we discussed setting something up so the fraudulent applicants would return to the bank to pick up the money. Thomas faxed us an affidavit to sign and have witnessed. While we were in the process of faxing the affidavit back, another call came in. Marquette Bank in Illinois had just accepted an application from someone using my husband's name and social security number. This was for a five thousand ($5,000.00) personal loan. I told this fraud investigator about the other two applications and the affidavit we were faxing to Bank One. These three fraudulent applications were made within a two hour period (3:00–5:00 P.M. EST) and they totaled forty-five thousand dollars ($45,000.00).

After we faxed the affidavit back to Thomas Retkowski at Bank One, I continued to work on the police report. At 8:00 P.M. we received a phone call from an Illinois detective informing us that a suspect had been arrested as he left Bank One. The suspect had five thousand dollars ($5,000.00) cash and two-five thousand dollar bank checks ($10,000.00) made payable to my husband's name. The money was recovered when the suspect was arrested. The suspect was also found to have an Illinois driver's license and an Illinois State Identification Card with his own picture on it, but my husband's name and social security number.

I called the Federal Trade Commission the following day and told Kathleen Lund that a suspect had been apprehended in Illinois. I gave her the detectives' names and the case number for her records. I continued to type our police report, and I continued to try to notify the merchants listed on the credit reports. In our mail on November 19, 1999, was a letter from PrimeCo, a cellular communication company, notifying us that a cell phone account had been established in Illinois using my husband's name and social security number. I called PrimeCo, at the number they provided in the letter, to let them know that we had not established the account. PrimeCo's fraud department immediately canceled the service to the cell phone, offered to provide the detectives with a copy of the application made to open the account, and said the detectives could obtain ALL of the outgoing numbers that were called from the fraudulent cell phone. The detectives needed to submit this request in writing on police letterhead stationary. I called the detectives to give them this information, and I was told they ran the fingerprints of the suspect who had been arrested the previous day. This suspect had 17 aliases and multiple priors. A preliminary hearing was set for November 20, 1999, and the detective said he would let me know what happened at the hearing.

I continued to make phone calls to try to resolve this nightmare when I learned that the suspect was released on a signature bond at the preliminary hearing. Words can't even begin to describe the horror I felt knowing that a suspect with seventeen aliases, multiple priors and an extensive criminal background was released on a signature bond in his own recognizance. The hearing was in Cook County, Illinois and the Judge was Thomas Panicki. I was also told that when this suspect was arrested he had stated to the detectives: ''I didn't use a gun, I didn't use a knife, call my lawyer I will plead guilty and they will put me on probation''. It was appalling for me to realize the criminals commit these crimes with a premeditated methodology that accomplishes their criminal intent with the least possible risk for the criminal, if apprehended, serving jail time. The criminals are still committing bank robbery, fraud, identity theft, forgery and a litany of other criminal acts, but because a traditional weapon was not used they face probation instead of incarceration. These criminals are using weapons nonetheless, their weapon is technology. It was technology that provided these criminals with our personal information, it was technology that produced the fraudulent documents used to obtain the Illinois drivers license and State Identification Card. It was technology used with criminal intent that thrust us into the nightmare of identity theft. It was technology that provided these criminals with my husbands previous employment information and employers address which were then used on fraudulent applications. This same technology, properly implemented and with appropriate safeguards, can be utilized to circumvent the criminals' fraudulent intentions.

It was the consumer profile of our spending habits established by the prior pattern of activity on our KeyBank Mastercard that prompted KeyBank to call us about the "unusual level of activity on our credit card." This same consumer profile technology can also be used by the credit reporting agencies to recognize an "unusual pattern of activity". Our credit reports, as a result of fraudulent activity, contained 30 inquiries in 60 days, yet our consumer profile showed fewer than 30 inquiries in 20 years. Our consumer profile showed we had resided at the same address for 20 years, yet the addresses listed on our credit reports, as a result of fraudulent applications, changed six times in 2 months. It is imperative that a system of "checks and balances" be implemented and adhered with by the credit reporting agencies.

As our Identity Theft saga continued we requested and received, from some cooperative merchants, copies of the applications that were made fraudulently. These applications contained numerous blatant errors that should have alerted the merchants and the banks that something was amiss. One example is an application that was made to purchase a Ford Expedition. This vehicle was purchased using my husband's name along with the name of a co-buyer. These two men presented themselves to the car dealership as residing together, yet on the application one man filled out the address as N. Grand and the other put W. Grand. On this same application the employer's phone number is listed with an area code of 300, this area code is not a valid area code in the continental United States. Our last name was misspelled on the application and on the fax from the lender approving the loan. On this same application the 60 month 60,000 mile extended warranty was purchased showing a cost of $695.00 on the application. When this figure was carried over to the debit column to determine the amount of credit to be extended it was entered as $1,695.00. In spite of these GLARING discrepancies this loan was approved and these two men purchased a Ford Expedition using our credit. If this was transaction was processed using due diligence and an iota of common sense these blatant discrepancies would have been caught. The possibility does exist that these criminals made the purchase through a car salesman, car dealership and lender that were co-conspirators, but I think that is a remote possibility. I do firmly believe that sloppy business practices substantially contribute to the criminal's ability to successfully defraud merchants and lenders. It was due diligence that was exercised by a salesperson in an Illinois furniture store that prevented the extension of credit to purchase furniture. The salesperson realized that "something wasn't right" after scrutinizing the credit application. Credit was not extended by the furniture store and the criminal was thwarted in this fraudulent attempt. I think this is a good example of how good business practices will diminish fraud.

We also were able to determine from pictures we received from the car merchants that the criminals who purchased the vehicles were not the same persons as the suspect who was apprehended leaving BankOne. We have been victimized by an Identity Theft ring which operates in an organized and insidious manner. The detectives told us that the criminals know when the fraud alerts on our credit reports will expire and if we fail to reactivate the fraud alerts our information will be recirculated through the ring again. We will have to keep fraud alerts on our credit reports for the rest of our lives. So, in the future, when my husband and I apply for any credit we will have to explain this nightmare to the lender, hope they believe us and don't perceive us as the criminals.

Our efforts to restore our good names and good credit have been extensive. I have made hundreds of phone calls, I've met with our Congressman (Steve LaTourette), I've sent dozens of notarized, certified, return receipt requested letters to the merchants informing them that the applications they received were fraudulent. We have submitted numerous affidavits, notarized statements, and notarized handwriting samples. We have filled out over twenty different sets of forms and statements in order to comply with the merchants requests for further information. It's like filling out your income tax return twenty different times, using twenty different forms, and following twenty different sets of instructions. I strongly suggest that a standardized, uniform protocol be established so a victim of Identity Theft can fill out one set of papers which should include a notarized affidavit, a notarized handwriting sample, and a notarized statement that will be universally accepted by the merchants and lenders.

A sad irony exists with Identity Theft: The criminal is assumed innocent until proven guilty, but the Identity Theft victim is assumed guilty until proven innocent. The criminal can have a public defender appointed to protect his legal rights, yet if we need to hire an attorney to assist in clearing our names we will be paying substantial legal fees out of pocket.

We have exhausted all known resources in an effort to clear our names and restore our credit. I've met with numerous police officers, I've met with FBI Agents,

I've met with a Victim's Assistance Program in our home state, and I've contacted a Victim Advocacy Program in Illinois. I've spoken to prosecuting attorneys, and sent packages of information to State's Attorneys. I was told by an assistant state prosecutor in Illinois: "No one in the state of Illinois serves jail time for non-violent financial crimes." This prosecutor was not even aware that Illinois has an Identity Theft Statute in the Revised Code. I've begged, pleaded and cajoled to try and obtain a Federal Investigator and a United States' Attorney to take our case. Identity Theft cases encompass numerous geographic areas and requires a Federal investigator and Federal prosecution. The detectives in the community where the suspect was apprehended are limited to investigating crimes within their geographic boundary, yet the same criminal is committing the same crime a few towns away. It was suggested that I submit police reports in each community where a merchant was defrauded, not an easy task from 350 miles away.

In spite of the efforts of my husband and myself to acquire Federal intervention into our case, it was the actions of Senator Jon Kyl and James McDermond of his staff, that resulted in the United States Secret Service and Postal Inspection Service initiating a Federal investigation.

I have logged over 400 hours of time trying to clear our names and restore our good credit. Words are unable to adequately express the gamut of emotions that we have experienced as victims. The impact of being a victim of Identity Theft is all encompassing. It affects you physically, emotionally, psychologically, spiritually and financially. This has truly been a life altering experience.

In spite of the extensive time and effort we have logged in trying to resolve this, we now have adverse ratings on our credit reports. We are also receiving phone calls from collection specialists wanting to know why we are overdue on the payments for our Lincoln Navigator and our Ford Expedition. I try to nicely explain to these collection specialists that we are victims of Identity Theft and we did not purchase these vehicles. I then provide them with the name and phone number of the detective, the case number and the reference number assigned by the Federal Trade Commission. I strongly suggest they not call me back unless they provide whatever information they may have to assist in the investigation. I always end my conversation with the collection specialist by saying: "It's amazing to me that you can find the real Mr. & Mrs. Mitchell when you want to collect your money, too bad you didn't find the real Mr. & Mrs. Mitchell before you loaned out the money."

Identity Theft has become a national epidemic. Banks and merchants are being defrauded out of billions of dollars each year by Identity Theft criminals. We all pay the price through the higher cost of consumer goods, and higher interest rates on loans and credit cards. This epidemic must be stopped. The compromising of real identities is now the weakest link in the chain of financial transactions. The credit that has been extended using our identities fraudulently exceeds $111,000.00. Unfortunately for us, this saga is far from over. Once you become a victim of Identity Theft your life is forever changed. We still feel like we are "waiting for the other shoe to drop." We do not know how many more accounts may still be outstanding, we do not know if a collection specialist is calling when our phone rings, we do not know if our good names and financial reputations will ever be truly restored. We need to be pro-active in the fight against Identity Theft and fraud and we need to impose mandatory jail sentences on criminals convicted of Identity Theft crimes.

"He that filches from me my good name robs me of that which not enriches him and makes me poor indeed." (*Shakespeare—Othello*)

I've attached a list of personal recommendations for your review. I thank you for your time and consideration and I truly hope you never walk in the shoes of an Identity Theft Victim.

The following are my 15 recommendations:

1. Victims of Identity Theft need to know to call the FTC @ (877–438–4338). The general public needs to know the Federal Trade Commission is the National Clearinghouse for Identity Theft.

2. The general public, police departments, law enforcement agencies, state prosecutors and judges need to know that a Federal Identity Theft and Deterrence Law is in effect making Identity Theft a Federal offense. (Title 18 US—Section 1028).

3. Since Identity Theft is a Federal Offense, investigations need to be handled by Federal Investigators, and prosecutions handled by U.S. attorneys. A good law needs adequate resources for investigation and prosecution.

4. Criminals convicted under the Identity Theft Laws should be prosecuted to the fullest extent of the Federal penalties and serve mandatory jail time when convicted.

5. Social Security numbers should not be used as identification numbers. The social security number should not appear on drivers licenses, on medical insurance

cards, on student identification cards, or on any other documents other than income tax returns and wage earnings statements. Identification numbers other than the social security numbers can be assigned.

6. Credit Reporting Agencies must verify the accuracy of the information received prior to posting information on credit reports. The credit reporting agencies can use available technology to "red-flag" information that does not fit the profile of the consumers' previous spending habits. Change of addresses need to be verified by the Credit Reporting Agencies prior to changing the address on the consumers' credit report. The information disseminated by the credit reporting agencies to the various lenders and merchants making credit inquiries is perceived by these banks and merchants as accurate because "it came from the credit bureau". It seems incongruous to have banks and merchants rely on the information appearing on credit reports when this information has been entered without any verification of accuracy.

7. Banks, lenders, merchants, car dealerships etc. need to use due diligence in scrutinizing the information received on loan applications for inaccuracies and blatant errors. Applications for credit have been approved with only the social security number matching, spelling of name was incorrect, address was changed, birth date was wrong, yet the loan was approved. Due diligence needs to be exercised at ALL steps of the loan process to reduce the occurrence of fraud.

8. The Department of Motor Vehicles in each state should use available technology to cross-reference the information in their data bases to ensure that a license cannot be issued in another state fraudulently with the same name and social security number as a valid license in another state. Regulations prohibiting the Department of Motor Vehicles from selling information should be enacted and enforced. The same applies f6r state issued ID cards.

9. The utilization of Bio-Metric technology, which is currently available, allowing a fingerprint, palm print or voice recognition system to be used as confirmation of identification will substantially reduce the current epidemic of credit fraud and identity theft.

10. Establish a standardized, universally accepted national protocol for victims of Identity Theft to follow. The bona fide victim should have to fill out one set of documents containing a notarized affidavit, a police report, a notarized handwriting sample and whatever other documentation may be necessary for the victim to be able to submit copies to each merchant.

11. Require banks to notify consumers to place fraud alerts on their credit reports if any of the consumers account or credit card information is compromised and used fraudulently.

12. Educate the local law enforcement authorities regarding Identity Theft. Provide the law enforcement officers who are taking police reports from victims on credit card fraud or Identity Theft with the materials needed to provide the victims with the information to contact the Federal Trade Commission, and the credit reporting agencies to place fraud alerts.

13. Impose financial penalties on merchants who, through their own carelessness and lack of good business practices, abet the criminals committing financial fraud.

14. Require the credit reporting agencies place the fraud alerts in bold typeface in a prominent position on the first page of a consumers credit report to reduce the chance of the alert being overlooked.

15. Eliminate advance checks and pre-approval solicitations being sent through the mail. The banks can mail a notice for the customer to obtain cash advance checks by coming into the bank to pick them up.

Senator KYL. I am now going to call the other two witnesses before us, Mr. Gregory Regan, Special Agent in Charge of the Financial Crimes Division of the U.S. Secret Service, and Ms. Jodie Bernstein, Director of the Bureau of Consumer Protection of the Federal Trade Commission.

Now, we have written statements from both of you and they will, of course, be included in the record. If you could summarize the statements, I would appreciate that, and then we will have some questions for you.

Mr. Regan.

PANEL CONSISTING OF GREGORY REGAN, SPECIAL AGENT IN CHARGE, FINANCIAL CRIMES DIVISION, U.S. SECRET SERVICE, WASHINGTON, DC; AND JODIE BERNSTEIN, DIRECTOR, BUREAU OF CONSUMER PROTECTION, FEDERAL TRADE COMMISSION, WASHINGTON, DC

STATEMENT OF GREGORY REGAN

Mr. REGAN. Yes, sir, thank you very much, Mr. Chairman. Mr. Chairman, members of the subcommittee, thank you for the opportunity to address the subcommittee concerning the subject of identity theft and the Secret Service's efforts to combat this problem.

My name is Gregory Regan and I am the Special Agent in Charge of the Financial Crimes Division for the U.S. Secret Service. A number of things have changed since the Secret Service last testified on this subject on April 1, 1998, before the Banking, Finance, and Urban Affairs Subcommittee. On behalf of the Secret Service, I would like to thank the subcommittee, and in particular the chairman, for taking a leadership role to effect this change.

This subcommittee was instrumental in directing the Federal Government's efforts to address this very serious problem. At a time when very little attention was being paid to identity theft victims, Senator Kyl was at the forefront. His efforts created an increased congressional awareness to their plight. In addition, he became a leading advocate for legislative change. His actions resulted in a concerted effort by both Congress and Federal law enforcement to address this problem.

We are proud to say that members of the Secret Service worked hand-in-hand with Senator Kyl's staff in drafting legislation which provided increased protection for the victims of identity theft through enhancements to 18 U.S.C. 1028. These enhancements became part of Senate bill 512, entitled The Identity and Assumption Deterrence Act, which was signed into law in October 1998.

The law accomplished four things simultaneously. First, it identified people whose credit had been compromised as true victims. Historically, with financial crimes such as bank fraud or credit card fraud, the victim identified by statute was the person, business, or financial institution that lost the money. All too often, the victims of identity theft whose credit was destroyed were not even recognized as victims. This is no longer the case.

Second, the law established the Federal Trade Commission as the one central point of contact for these victims to report all instances of identity theft. This collection of all ID theft cases allows for the identification of systemic weaknesses and the ability of law enforcement to retrieve investigation data at one central location. It further allows the FTC to provide people with the information and assistance they need in order to take the steps necessary to correct their credit records.

Third, this law provided increased sentencing potential and enhanced asset forfeiture provisions. These enhancements help to reach prosecutorial thresholds and allow for the repatriation of funds to victims.

Lastly, and probably most important in today's technology, this law closed a loophole in 18 U.S.C. 1028 by making it illegal to steal another person's personal identification information with the intent

to commit a violation. Previously, under section 1028, only the production or possession of false identity documents was prohibited. With advances in technology such as e-commerce and the Internet, criminals today do not need actual documents to assume an identity.

As we enter the new millennium, the strength of the financial industry has never been greater. A strong economy, burgeoning use of the Internet, and advanced technology, coupled with increased spending, has led to fierce competition within the financial sector. Although this provides benefits to the consumer through readily available credit and consumer-oriented financial services, it also creates a target-rich environment for today's sophisticated criminals, many of whom are organized and operate across international borders.

In addition, information collection has become a common by-product of the newly emerging e-commerce. Internet purchases, credit card sales, and other forms of electronic transactions are being captured, stored and analyzed by entrepreneurs intend on increasing their market share. This has led to an entirely new business sector being created which promotes the buying and selling of personal information.

A recently publicized Internet fraud investigation by the Secret Service, Department of Defense, Postal Inspection Service and the Social Security Administration Inspector General's office highlighted the ease with which criminals can obtain personal information through public sources. These defendants had access to Web sites that published the promotion lists of high-ranking military officers. The site further documented personal information on these officers that was used to fraudulently obtain credit, merchandise and other services.

In this particular case, the financial institution, in an effort to operate in a consumer-friendly manner, issued credit over the Internet in less than a minute. Approval for credit was granted after conducting a credit check for the applicant, who provided a true name and matching true Social Security number. All other information provided, such as the date of birth, address and telephone number that could have been used for further verification, was fraudulent. The failure of this bank to conduct a more comprehensive verification process resulted in substantial losses, and more importantly a long list of high-ranking military officers who became victims of identity fraud.

The Internet provides the anonymity that criminals desire. Now, with just a laptop and modem, criminals are capable of perpetrating a variety of financial crimes without identity documents through the use of stolen personal information. The Secret Service has investigated several cases where cyber criminals have hacked into Internet merchant sites and stolen the personal information and credit card account numbers of their customers. These account numbers are then used with supporting personal information to order merchandise, which is then sent throughout the world. Most account-holders are not aware that their credit card account has been compromised until they receive their billing statements.

Cyber criminals are also using information hacked from sites on the Internet to extort money from companies. It is not unprece-

dented for international hackers to hack into business accounts, steal thousands of credit card account numbers, along with the accompanying personal identifiers, then threaten the companies with exposure unless the hackers are paid a substantial amount of money.

The Secret Service continues to attack identity theft by aggressively pursuing our core violations. As stated earlier, identity theft and the use of false identification has become an integral component of most financial criminal activity. In order to be successful in suppressing identity theft, we believe law enforcement agencies should continue to focus their energy and available resources on the criminal activities which incorporate the misuse or theft of identification information.

The Secret Service investigative program focuses on three areas of criminal schemes within our core expertise. First, the Secret Service emphasizes the investigation of counterfeit instruments. By counterfeit instruments, I refer to counterfeit currency; counterfeit checks, both commercial and government; counterfeit credit cards; counterfeit stocks or bonds; and virtually any negotiable instrument that can be counterfeited. Many of these schemes would not be possible without the compromise of innocent victims' financial identifiers.

Second, the Secret Service targets organized criminal groups which are engaged in financial crimes on both a national and international scale. Again, we see many of these groups, most notably the Nigerian and Asian organized criminal groups, prolific in their use of stolen financial and personal information to further their financial crime activity.

And, last, we focus our resources in areas that have the most deleterious effect on the communities in which we work. We also work very closely with both Federal and local prosecutors to ensure that our investigations are relevant, topical and prosecutable under existing guidelines. No area today is more relevant or topical than that of identity theft. Automated teller machines, electronic commerce, online banking, online trading, smart cards, all once considered futuristic concepts, are now a reality. Each of these technology lends themselves to creating a faceless society.

One innovation which appears to address the problem of identity verification in Internet commerce has been developed and introduced by a member of the financial community. This new product is the first commercial venture by the credit card industry to provide the public with an online authentication process using chip technology in encryption. Although this product may not end credit card fraud on the Internet, it is the first step in providing a more secure environment in which to conduct Internet commerce.

In addition, under the direction of the President, a national summit on the subject of identity theft will commence next week, on March 15, 2000, at the Omni Shoreham Hotel here in Washington, to address this very serious issue.

As you have heard in this testimony, some very positive steps are being taken to address and combat identity theft. The Secret Service will always encourage both business and law enforcement to work together to develop an environment in which personal information is securely guarded. In this age of instant access, knowl-

edge is power. We cannot allow today's criminals to abuse the very systems which were created for the betterment of society.

The emotional toll on the lives of those whose identity has been compromised cannot be fully accounted for in dollars and cents. We do not believe, nor are we in the business of inhibiting the free flow of information so vital to a free society. We do, however, believe that those identified as misusing personal information for criminal purposes should be subject to punishment commensurate with the crime. The Secret Service acknowledges identity theft as a very real problem and pledges its support in the Federal Government's efforts to eliminate it.

This concludes my testimony and I would be happy to answer any questions you have, sir.

Senator KYL. Thank you very much, Mr. Regan. That is great. I will be asking some questions in a moment.

[The prepared statement of Mr. Regan follows:]

PREPARED STATEMENT OF GREGORY REGAN

Mr. Chairman, members of the subcommittee, thank you for the opportunity to address this subcommittee concerning the subject of identity theft and the Secret Service's efforts to combat this problem.

My name is Gregory Regan, and I am the Special Agent in Charge of the Financial Crimes Division of the United States Secret Service.

A number of things have changed since the Secret Service last testified on this subject on April 1, 1998, before the Banking, Finance, and Urban Affairs Subcommittee. On behalf of the Secret Service, I would like to thank this subcommittee, and in particular, the chairman for taking a leadership role to effect this change. This subcommittee was instrumental in directing the Federal Government's efforts to address this very serious problem.

At a time when very little attention was being paid to identity theft victims, Senator Kyl was at the forefront. His efforts created an increased congressional awareness to their plight. In addition, he became a leading advocate for legislative change. His actions resulted in a concerted effort by both Congress and Federal law enforcement to address this problem.

We are proud to say that members of the Secret Service worked hand in hand with Senator Kyl's staff in drafting legislation which provided increased protection for the victims of identity theft through enhancements to Title 18 United States Criminal Code, Section 1028. These enhancements became part of Senate bill 512, entitled The Identity Theft and Assumption Deterrence Act, which was signed into law in October 1998.

This law accomplished four things simultaneously. First, it identified people whose credit had been compromised as true victims. Historically with financial crimes such as bank fraud or credit card fraud, the victim identified by statute, was the person, business or financial institution that lost the money. All too often the victims of identity theft whose credit was destroyed, were not even recognized as victims. This is no longer the case.

Second, this law established the Federal Trade Commission (FTC) as the one central point of contact for these victims to report all instances of identity theft. This collection of all ID theft cases allows for the identification of systemic weaknesses and the ability of law enforcement to retrieve investigative data at one central location. It further allows the FTC to provide people with the information and assistance they need in order to take the steps necessary to correct their credit records.

Third, this law provided increased sentencing potential and enhanced asset forfeiture provisions. These enhancements help to reach prosecutorial thresholds and allow for the repatriation of funds to victims.

Lastly, this law closed a loophole in Title 18, United States Code, 1028 by making it illegal to steal another person's personal identification information with the intent to commit a violation. Previously, under Section 1028 only the production or possession of false identity documents was prohibited. With the advances in technology such as e-commerce and the Internet, criminals today do not need actual documents to assume an identity.

We believe the passage of this legislation was the catalyst needed to bring together both the Federal and State Government's resources, in a focused and unified

response to the identity theft problem. Today, law enforcement, regulatory and community assistance organizations have joined forces through a variety of working groups, task forces, and information sharing initiatives to assist victims of identity theft. Victims no longer have to feel abandoned, with no where to turn.

Policies and procedures are being initiated to expedite the reporting of this crime. Civil remedies are being created allowing for victims to seek restitution. The Secret Service victim-witness assistance program aids identity theft victims by providing resources and contact information for credit bureaus and service programs. The financial community continues to design and implement security measures which minimize the exploitation of true persons names and identification information.

The Secret Service has broad investigative responsibilities relating to financial crimes. Today, some type of false identification is a prerequisite for nearly all financial fraud crimes. False ID's provide anonymity to criminals and allow for repeat victimization of the same individual while perpetrating a variety of fraud schemes. Often, in their attempt to remain anonymous, criminals may randomly assume the identity of another individual through the creation of false identification documents. In these cases, the goal may not be to target an individual for the purposes of stealing his or her identity. Yet, by coincidence, that individual's identity has been compromised through the criminal's use of their personal identifiers.

False identification documents altered, counterfeited, or fraudulently obtained, are routinely used with loan and check fraud schemes, and almost all credit card fraud schemes. Ironically, the credit industry through capital investments over the past 10 years has strengthened the integrity of the system through security measures which effectively thwart some types of direct counterfeiting. Subsequently, criminals no longer simply create names and identities, they must more often rely on the identifiers of real people.

As we enter the new millennium the strength of the financial industry has never been greater. A strong economy, burgeoning use of the Internet and advanced technology, coupled with increased spending has led to fierce competition within the financial sector. Although this provides benefits to the consumer through readily available credit, and consumer oriented financial services, it also creates a target rich environment for todays sophisticated criminals, many of whom are organized and operate across international borders.

In addition, information collection has become a common by-product of the newly emerging e-commerce. Internet purchases, credit card sales, and other forms of electronic transactions are being captured, stored, and analyzed by entrepreneurs intent on increasing their market share. This has led to an entirely new business sector being created which promotes the buying and selling of personal information.

With the advent of the Internet, companies have been created for the sole purpose of data mining, data warehousing, and brokering of this information. These companies collect a wealth of information about consumers, including information as confidential as their medical histories.

Consumers routinely provide personal, financial, and health information to companies engaged in business on the Internet. Consumers may not realize that the information they provide in credit card applications, loan applications, or with merchants they patronize, are valuable commodities in this new age of information trading.

Data collection companies like all businesses are profit motivated, and as such, may be more concerned with generating potential customers rather than the misuse of this information by unscrupulous individuals. This readily available personal information in conjunction with the customer friendly marketing environment has presented ample opportunities for criminals intent on exploiting the situation for economic gain.

We have investigated numerous cases where criminals have used other people's identities to purchase everything from computers to houses. Financial institutions must continually practice due diligence lest they fall victim to the criminal who attempts to obtain a loan or cash a counterfeit check using someone else's identity.

As financial institutions and merchants become more cautious in their approach to "hand to hand" transactions the criminals are looking for other venues to compromise. Today, criminals need look no further than the Internet.

For example, a recently publicized Internet fraud investigation by the Secret Service, Department of Defense, Postal Inspection Service, and the Social Security Administration Inspector General's Office highlighted the ease with which criminals can obtain personal information through public sources. These defendants accessed a Web site that published the promotion list of high ranking military officers. This site further documented personal information on these officers that was used to fraudulently obtain credit, merchandise, and other services.

In this particular case the financial institution, in an effort to operate in a consumer friendly manner issued credit over the Internet in less than a minute. Approval for credit was granted after conducting a credit check for the applicant who provided a "true name" and matching "true Social Security number". All other information provided such as the date of birth, address and telephone number, that could have been used for further verification, was fraudulent. The failure of this bank to conduct a more comprehensive verification process resulted in substantial losses and more importantly a long list of high ranking military officers who became victims of identity fraud.

The Internet provides the anonymity criminals desire. In the past, fraud schemes required false identification documents, and necessitated a "face to face" exchange of information and identity verification. Now with just a laptop and modem, criminals are capable of perpetrating a variety of financial crimes without identity documents through the use of stolen personal information.

The Secret Service has investigated several cases where cyber criminals have hacked into Internet merchant sites and stolen the personal information and credit card account numbers of their customers. These account numbers are then used with supporting personal information to order merchandise which is then sent throughout the world. Most account holders are not aware that their credit card account has been compromised until they receive their billing statement.

Time and time again, criminals have demonstrated the ability to obtain information from businesses conducting commerce on the Internet. This information has been used to facilitate account takeover schemes and other similar frauds. It has become a frightening reality that one individual can literally take over another individual's credit card account and or bank account without the true subscriber's knowledge.

Cyber criminals are also using information hacked from sites on the Internet to extort money from companies. It is not unprecedented for international hackers to hack into business accounts, steal thousands of credit card account numbers along with the accompanying personal identifiers, then threaten the companies with exposure unless the hackers are paid a substantial amount of money.

The Secret Service continues to attack identity theft by aggressively pursuing our core violations. It is by the successful investigation of criminals involved in financial and computer fraud that we are able to identify and suppress identity theft.

As stated earlier, identity theft, and the use of false identification has become an integral component of most financial criminal activity. In order to be successful in suppressing identity theft we believe law enforcement agencies should continue to focus their energy and available resources on the criminal activities which incorporate the misuse or theft of identification information.

The Secret Service has achieved success through a consistent three tiered process of aggressive pro-active investigations, identification of systemic weaknesses, and partnerships with the financial sector to adopt fixes to these weaknesses.

The Secret Service's investigative program focuses on three areas of criminal schemes within our core expertise. First, the secret service emphasizes the investigation of counterfeit instruments. By counterfeit instruments, I refer to counterfeit currency, counterfeit checks, both commercial and government, counterfeit credit cards, counterfeit stocks or bonds, and virtually any negotiable instrument that can be counterfeited. Many of these schemes would not be possible without the compromise of innocent victims financial identities.

Second, the Secret Service targets organized criminal groups which are engaged in financial crimes on both a national and international scale. Again we see many of these groups, most notably the Nigerian and Asian organized criminal groups, prolific in their use of stolen financial and personal information to further their financial crime activity.

And last, we focus our resources on cases that have the most deleterious effect on the communities in which we work. The Secret Service works in concert with the state, county, and local police departments to ensure our resources are being targeted to those criminal areas that are of a high concern to the local citizenry. Further, we work very closely with both Federal and local prosecutors to ensure that our investigations are relevant, topical and prosecutable under existing guidelines. No area today is more relevant or topical than that of identity theft.

It has been our experience that the criminal groups involved in these types of crimes routinely operate in a multi- jurisdictional environment. This has created problems for local law enforcement who generally act as the first responders to their criminal activities. By working closely with other Federal, state, and local law enforcement, as well as international police agencies we are able to provide a comprehensive network of intelligence sharing, resource sharing, and technical expertise which bridges jurisdictional boundaries.

This partnership approach to law enforcement is exemplified by our financial crimes task forces located throughout the country. Each of these task forces pools the personnel and technical resources and to maximize the expertise of each participating law enforcement agency. A number of these task forces are focused on the Nigerian criminal element operating in this country. As mentioned earlier, this particular ethnic criminal group has historically been involved in a myriad of financial crimes, which incorporate false identification and identity theft.

In addition to our inter-dependant working relationship with law enforcement on all levels, our partnership with the private sector has proved invaluable. Representatives from numerous commercial sectors to include the financial, telecommunications, and computer industries have all pledged their support in finding ways to ensure consumer protection while minimizing corporate losses. The Secret Service has entered into several cooperative efforts with members of the financial sector to address challenges posed by new and emerging technologies. These initiatives have created some new and innovative approaches to identification verification in business.

Automated teller machines, e-commerce, online banking, online trading, smart cards, all once considered futuristic concepts, are now a reality. Each of these technologies lends themselves to creating a "faceless society". In order for businesses to be successful, they can no longer rely upon personal contact as a means of identity verification.

One innovation which appears to address the problems of identity verification for Internet commerce has been developed and introduced by a member of the financial community. This new product is the first commercial venture by the credit card industry to provide the public with an online authentication process using chip technology and encryption. Although this product may not end credit card fraud on the Internet, it is the first step in providing a more secure environment in which to conduct Internet commerce.

Efforts such as these provide a foundation by which law enforcement and the private sector can build upon. By applying the technologies used in this product and others being developed for the same purpose, we can systemically eliminate the weaknesses in our economic infrastructure, which allow for the misuse of personal information.

In conjunction with these technological advances, the Secret Service is actively involved with a number of government sponsored initiatives. At the request of the Attorney General, the Secret Service joined an interagency identity theft subcommittee that was established by the Department of Justice. This group which is made up of Federal and state law enforcement, regulatory agencies, and professional agencies meets regularly to discuss and coordinate investigative and prosecutive strategies as well as consumer education programs.

In addition, under the direction of the President, the Treasury Department, with the assistance of the Secret Service, has been tasked with convening a national, summit on the subject of identity theft. The purpose of this summit is to bring together various Federal, state, and private sector entities to discuss and develop policies that will help prevent identity theft crimes. This summit will commence next week on March 15, 2000, at the Omni Shoreham Hotel, herein Washington, DC.

As you have heard in this testimony some very positive steps are being taken to address and combat identity theft. The Secret Service will always encourage both business and law enforcement to work together to develop an environment in which personal information is securely guarded. In this age of instant access, knowledge is power. We cannot allow todays criminals to abuse the very systems which were created for the betterment of society. The emotional toll on the lives of those whose identity has been compromised cannot be fully accounted for in dollars and cents. It is all of our responsibilities to protect personal information.

We do not believe, nor are we in the business of inhibiting the free flow of information so vital to a free society. We do, however, believe that those identified as misusing personal information for criminal purposes should be subject to punishment commensurate with the crime. The concepts of criminal prosecution for the perpetrators, restitution for the victims, and ethical responsibilities for those earning a living through the use of personal information are noble goals.

The Secret Service acknowledges that identity theft is a very real problem and pledges its support in the Federal Government's efforts to eliminate it.

This concludes my prepared statement. I would be happy to answer any questions that you or any other member of the subcommittee may have. Thank you.

GREGORY J., REGAN, SPECIAL AGENT IN CHARGE FINANCIAL CRIMES DIVISION U.S. SECRET SERVICE

Mr. Gregory J. Regan was appointed Special Agent in Charge of the Financial Crimes Division on January 3, 1999. Prior to this appointment, he served as the Assistant Special Agent in Charge of the Richmond Field Office.

Mr. Regan began his law enforcement career in 1980 as a Special Agent with the Naval Investigative Service. In 1982, Mr. Regan was appointed as a Special Agent with the U.S. Secret Service and assigned to the New York Field Office. His subsequent career assignment included duty on the Vice Presidential Protective Division, a prior assignment to Financial Crimes Division, the Office of Congressional Affairs, and the Counterfeit Division.

A native of Brooklyn, New York, Mr. Regan received a Bachelor of Arts Degree from St. John's University in New York. He is married to the former Margaret Stokey of Westbury, New York and they have five children.

Mr. Regan is the Chairman of the Law Enforcement Advisory Committee for the International Association of Financial Crimes Investigators; and is a member of the Investigative Operations Committee for the International Association of Chiefs of Police.

Throughout his tenure with the U.S. Secret Service, Mr. Regan has been the recipient of numerous awards to include the law enforcement officer of the year award from the International Association of Credit Card Investigators.

Senator KYL. Let's hear now from Ms. Jodie Bernstein.

STATEMENT OF JODIE BERNSTEIN

Ms. BERNSTEIN. Thank you, Senator Kyl. As you said, I am Jodie Bernstein and I am the Director of the Bureau of Consumer Protection at the Federal Trade Commission. And I wanted to thank you particularly for including us in this hearing and giving us the opportunity to present the Commission's testimony on these problems.

I would also like to introduce one of our staff, Beth Grossman, who has been very much involved, in fact critical, to the development of the FTC's initiatives following the passage of the Act.

I would acknowledge also, as Ms. Mitchell did, Kathleen Lund, of our staff, who was Ms. Mitchell's counselor. And she doesn't often get the opportunity to be acknowledged for the really wonderful work that she did in connection with an individual case and was pleased to be able to attend this hearing.

I will try to summarize my testimony, also, very briefly. And as Ms. Mitchell said so eloquently, identity theft causes significant and ongoing problems for its victims. Identity thieves can run up debts in the tens of thousands of dollars under their victims' names. Even when the victim is not legally liable for the debts, the consequences are often considerable. A victim's credit history is often scarred, and he or she typically must spend hundreds of hours, sometimes over the course of months and even years, contesting bills and straightening out credit reporting errors.

The passage of the Act was an important step in combatting identity theft and in helping its victims. The Act, as you so correctly anticipated, strengthened the criminal laws against identity theft and recognized that the individual whose identity has been stolen is as much a victim as the financial institutions that may have borne most of the monetary loss.

The Act also provided a framework for the FTC's new and unique program to assist victims of identity theft. The FTC's consumer assistance effort has three principal components, and we have some graphics to help illustrate it.

First, we have established an identity theft hotline that consumers can call toll-free at, as you see, 887–IDTHEFT. The hotline provides the public with a central place to call to report identity theft and to receive information on the steps to take if they become identity theft victims.

Second, we have another slide. We have a complaint clearinghouse, a database to track the reports that the FTC and other agencies receive about identity theft. The database will provide the FTC with information about the nature and extent of consumers' ID theft-related problems. Later this year, we plan to make the clearinghouse available to other law enforcement agencies through a secure Web-based interface.

Through this secure Web site, criminal investigative agencies like the Secret Service will be able to access the database of complaints from their desktop PC's to spot patterns of criminal activity that might not otherwise be apparent from isolated reports. We have built this database on the model of a different database that we developed that is called Consumer Sentinel. It is a network to track consumer fraud generally, and really Sentinel has been such a great success that we expect to have no less of an effort from this database.

Third, the Commission has launched a significant consumer education effort. We recently published a 21-page booklet, and I think we have copies of it here today as well. And it is called, as you know, "Identity Theft: When Bad Things Happen to Your Good Name." This booklet that was put together with the assistance of several Federal agencies is a comprehensive guide for consumers with information ranging from how consumers can protect their personal information to how to correct credit-related problems that may result from identity theft. Several other agencies have agreed to reproduce and distribute the booklet, which will be extremely helpful. We have produced a number of shorter, more targeted pieces as well.

The FTC also provides consumers with information through our identity theft Web site. The Web site, located at consumer.gov/idtheft, contains our publications, as well as the following: tips on what consumers can do to decrease the risk of becoming a victim, the steps consumers should take if they do become victims, information on recent identity theft cases and scams, lists and links to many of the State identity theft laws, links to other identity theft resources throughout the Government, and finally a public complaint form—and this has really been, I think, very useful—that allows consumers to submit reports of identity theft directly to our database at any time of the day or night. And because our database will have a record of their report, they can phone our call center during business hours for follow-up information.

Since we launched our toll-free number just a little over 3 months ago, we have been averaging over 400 calls a week from consumers. After a recent press release, the number of calls increased by about 25 percent. We expect that the volume of calls will continue to rise as more and more people know about the toll-free number. We anticipate that as it is more widely known, we are anticipating based on prior experience that we may be receiving more than 100,000 calls by next year.

Because our data collection efforts are new, though, we can't yet do extensive data analysis of the calls. Our basic complaint data, though—we have a little bit of analysis we have been able to do—shows that the most common forms of identity theft are as follows: first, credit card fraud. Fifty-five percent of the callers report that someone either opened up a credit card account in their name or, "took over" their existing credit card account.

Second, 25 percent report that utility service, such as telephone or cellular service, has been opened up in their name. About 15 percent report a checking or savings account has been opened in their name and/or that fraudulent checks had been written. Ten percent complain that an identity thief obtained a loan, such as a car loan, in their name.

Having succeeded in putting the basic components of the program in place, we are looking at new, additional ways that we can build on the foundation. And as we move forward, one focus will be on identifying ways we can work together with the private sector on this important issue. As the Identity Theft Act recognized, private companies, such as credit card issuers and credit bureaus, are essential to any effort to combat identity theft. Indeed, they are often, as Maureen said, in the best position to identify and prevent identity theft in the first place—and nothing is better than prevention—and to clear up fraudulent accounts opened in the consumer's name.

As you know, the Treasury Department is sponsoring a national summit on identity theft next week which will specifically address ways in which government, business leaders and consumers can forge partnerships to counter identity theft. The FTC has been assisting in organizing the summit. Both the chairman of the Commission and I will participate in it, and we are looking forward to the opportunity to explore new ways of addressing the growing problem.

Thank you, Mr. Chairman, again on behalf of the Commission, and we will be pleased to answer any of your questions.

[The prepared statement of Ms. Bernstein follows:]

PREPARED STATEMENT OF JODIE BERNSTEIN

Mr. Chairman Kyl, and members of the Subcommittee, I am Jodie Bernstein, Director of the Bureau of Consumer Protection, Federal Trade Commission ("FTC" or "Commission").[1] I appreciate the opportunity to present the Commission's views on the important issue of identity theft, and describe to you the Commission's achievements in implementing the Identity Theft and Assumption Deterrence Act.[2]

In my remarks today, I will discuss the growing phenomenon of identity theft, how the Commission has responded to identity theft, both in carrying out its duties under the 1998 Act and its general enforcement measures, and what we see as future challenges in eradicating identity theft.

I. IDENTITY THEFT: A GROWING PROBLEM

By now, many people have confronted, directly or through a third person, some form of identity theft: someone has used their name to open up a credit card account or someone has used their identifying information—name, social security number, mother's maiden name, or other personal information—to commit fraud or engage in other unlawful activities. Other common forms of identity theft include taking

[1] The views expressed in this statement represent the views of the Commission. My oral presentation and response to questions are my own, and do not necessarily represent the views of the Commission or any Commissioner.

[2] Pub. L. No. 105–318, 112 Stat. 3007 (1998) (codified at 18 U.S.C. § 1028).

over an existing credit card account and making unauthorized charges on it (typically, the identity thief forestalls discovery by the victims by contacting the credit card issuer and changing the billing address on the account); taking out loans in another person's name; writing fraudulent checks using another person's name and/or account number; and using personal information to access, and transfer money out of, another person's bank or brokerage account. In extreme cases, the identity thief may completely take over his or her victim's identity—opening a bank account, getting multiple credit cards, buying a car, getting a home mortgage and even working under the victim's name.[3]

Identity theft can arise from simple, low-tech practices such as stealing someone's mail or "dumpster diving" through their trash to collect credit card offers or obtain identifying information such as account numbers or social security numbers. There are also far more sophisticated practices at hand. In a practice known as "skimming," identity thieves use computers to read and store the information encoded on the magnetic strip of an ATM or credit card when that card is inserted through either a specialized card reader or a legitimate payment mechanism (*e.g.,* the card reader used to pay for gas at the pump in a gas station). Once stored, that information can be re-encoded onto any other card with a magnetic strip, instantly transforming a blank card into a machine-readable ATM or credit card identical to that of the victim.

The Internet has dramatically altered the potential impact of identity theft. Among other things, the Internet provides access to collections of identifying information gathered through both illicit and legal means. The global publication of identifying details that heretofore were available only to the few increases the potential misuse of that information. Similarly, Internet expands exponentially the ability for a third party to disseminate the identifying information, making it available for others to exploit. The recent reports of a Russian hacker gaining access to the names, addresses and credit card account numbers of hundreds of thousands of customers is an extreme example of the type of harm that can occur through the wholesale theft of identifying information. In this instance, the hacker posted the names and credit card numbers on a website, providing the wherewithal for others to commit identity theft by using those credit card numbers to make purchases.[4]

Anecdotes and news stories provide one indication of the growth of identity theft. Available statistics confirm this trend. The General Accounting Office, for example, reports that consumer inquiries to the Trans Union credit bureau's Fraud Victim Assistance Department increased from 35,235 in 1992 to 522,922 in 1997,[5] and that the Social Security Administration's Office of the Inspector General conducted 1,153 social security number misuse investigations in 1997 compared with 305 in 1996.[6] In 1999, the telephone hotline established by the Social Security Administration Inspector General received reports of almost 39,000 incidents of misuse of Social Security Numbers.[7]

For victims of identity theft, the costs can be significant and long-lasting. Identity thieves can run up debts in the tens of thousands of dollars under their victims' names. Even where the individual consumer is not legally liable for these debts,[8] the consequences to the consumer are often considerable. A consumer's credit history is frequently scarred, and he or she typically must spend numerous hours sometimes over the course of months or even years contesting bills and straightening out credit reporting errors. In the interim, the consumer victim may be denied loans, mortgages, a driver's license, and employment; a bad credit report may even prevent him or her from something as simple as opening up a new bank account at a time when other accounts are tainted and a new account is essential. Moreover,

---

[3] In at least one case, an identity thief reportedly even died using the victim's name, and the victim had to get the death certificate corrected. Michael Higgins, *Identity Thieves,* ABA Journal, October 1998, at 42, 47.

[4] John Markoff, *Thief Reveals Credit Card Data When Web Extortion Plot Fails,* N.Y. Times, January 10, 2000, at A1.

[5] Calls to this department included "precautionary" phone calls, as well as calls from actual fraud or identity theft victims.

[6] U.S. General Accounting Office, Identity Fraud: Information on Prevalence, Cost, and Internet Impact is Limited (May 1998). The Social Security Administration attributed the increase in investigations, in part, to the hiring of additional investigators.

[7] While we have created a database to capture information from complaints to our new toll-free Identity Theft Hotline (discussed in greater detail below), our data are still too limited to allow us to draw any significant conclusions about the extent of identity theft.

[8] The Fair Credit Billing Act, 15 U.S.C. §1601 *et seq.* and the Electronic Fund Transfer Act, 15 U.S.C. §1693 *et seq.* limit consumers' liability for fraudulent transactions in connection with credit and debit cards, respectively.

even after the initial fraudulent bills are resolved, new fraudulent charges may continue to appear, requiring ongoing vigilance and effort by the victimized consumer.

II. THE FEDERAL TRADE COMMISSION'S AUTHORITY

A. Overview

The FTC's mission is to promote the efficient functioning of the marketplace by protecting consumers from unfair or deceptive acts or practices and increasing consumer choice by promoting vigorous competition. The Commission's primary legislative mandate is to enforce the Federal Trade Commission Act ("FTC Act"), which prohibits unfair methods of competition and unfair or deceptive acts or practices in or affecting commerce.[9] With certain exceptions, the FTC Act provides the Commission with broad civil law enforcement authority over entities engaged in or whose business affects commerce,[10] and provides the authority to gather information about such entities.[11] The Commission also has responsibility under more than forty additional statutes governing specific industries and practices.[12]

Two of the Commission's specific statutory mandates are particularly relevant in the context of identity theft. The Fair Credit Billing Act and Fair Credit Reporting Act each provide important protections for consumers who may be trying to clear their credit records after having their identities stolen. The Fair Credit Billing Act, which amended the Truth in Lending Act, provides for the correction of billing errors on credit accounts and limits consumer liability for unauthorized credit card use.[13] The Fair Credit Reporting Act ("FCRA") regulates credit reporting agencies and places on them the responsibility for correcting inaccurate information in credit reports.[14] In addition, entities that furnish information to credit reporting agencies have obligations under the FCRA to ensure the accuracy of the information they report.[15] Finally, the FCRA limits the disclosure of consumer credit reports only to entities with specified "permissible purposes" (such as evaluating individuals for credit, insurance, employment or similar purposes) and under specified conditions (such as certifications from the user of the report).[16]

B. The commission's involvement in identity theft issues

As an outgrowth of its broader concern about financial privacy, the Commission has been involved in the issue of identity theft for some time. In 1996, the Commission convened two public meetings in an effort to learn more about identity theft, its growth, consequences, and possible responses. At an open forum convened by the Commission in August 1996, consumers who had been victims of this type of fraud, representatives of local police organizations and other federal law enforcement agencies, members of the credit industry, and consumer and privacy advocates discussed the impact of identity theft on industry and on consumer victims. Subsequent press coverage helped to educate the public about the growth of consumer identity theft and the problems it creates. In November 1996, industry and consumer representatives met again in working groups to explore solutions and ways to bolster efforts to combat identity theft.

Having developed a substantial base of knowledge about identity theft, the Commission testified before this subcommittee in May 1998 in support of the Identity Theft and Assumption Deterrence Act. Following the passage of the Act, the Commission testified again, in April 1999, before the House Subcommittee on Telecommunications, Trade and Consumer Protection and the Subcommittee on Finance and Hazardous Materials of the Commerce Committee. This latest testimony focused on identity theft in the financial services industry.

---

[9] 15 U.S.C. § 45(a).

[10] Certain entities such as banks, savings and loan associations, and common carriers as well as the business of insurance are wholly or partially exempt from Commission jurisdiction. *See* Section 5(a)(2) of the FTC Act, 15 U.S.C. § 45(a)(2), and the McCarran-Ferguson Act, 15 U.S.C. § 1012(b).

[11] 15 U.S.C. § 46(a).

[12] In addition to the credit laws discussed in the text, the Commission also enforces over 30 rules governing specific industries and practices, *e.g.*, the Used Car Rule, 16 C.F.R. Part 455, which requires used car dealers to disclose warranty terms via a window sticker; the Franchise Rule, 16 C.F.R. Part 436, which requires the provision of information to prospective franchisees; and the Telemarketing Sales Rule, 16 C.F.R. Part 310, which defines and prohibits deceptive telemarketing practices and other abusive telemarketing practices.

[13] 15 U.S.C. §§ 1601 *et seq.*

[14] 15 U.S.C. §§ 1681e, 1681i.

[15] 15 U.S.C. § 1681s–2.

[16] 15 U.S.C. § 1681–1681u.

C. The Identity Theft and Assumption Deterrence Act of 1998

The Identity Theft and Assumption Deterrence Act of 1998 ("Identity Theft Act" or "the Act") addresses identity theft in two significant ways. First, the Act strengthens the criminal laws governing identity theft. Specifically, the Act amends 18 U.S.C. § 1028 ("Fraud and related activity in connection with identification documents") to make it a federal crime to:

> knowingly transfer[] or use[], without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law.[17]

The second way in which the Act addresses the problem of identity theft is by focusing on consumers as victims.[18] In particular, the Act requires the Federal Trade Commission to develop a centralized complaint and consumer education service for victims of identity theft. More specifically, the Act directs that the Commission establish procedures to: (1) log the receipt of complaints by victims of identity theft; (2) provide identity theft victims with informational materials; and (3) refer complaints to appropriate entities, including the major national consumer reporting agencies and law enforcement agencies.[19]

III. CURRENT EFFORTS: THE FTC'S CONSUMER ASSISTANCE PROGRAM

In enacting the Identity Theft Act, Congress recognized that coordinated efforts are essential because identity theft victims often need assistance from both government agencies at the national and state or local level, and private businesses. Accordingly, the FTC's role under the Act is primarily one of managing information sharing among public and private entities. The goals of the FTC's information "clearinghouse". are fourfold: (1) to support criminal law enforcement efforts by collecting data in one central database and making referrals as appropriate[20]; (2) to provide consumers with information to help them prevent or minimize their risk of identity theft; (3) to streamline the resolution of the credit and financial difficulties consumers may have when they become victims of identity theft; and (4) to enable analysis of the extent of, and factors contributing to, identity theft in order to enrich policy discussions. In order to fulfill the purposes of the Act, the Commission has begun implementing a plan that centers on three principal components:

(1) *Toll-free telephone line.* The Commission has established a toll-free telephone number, 1–877–ID THEFT (438–4338), that consumers can call to report incidents of identity theft. Consumers who call the Identity Theft Hotline receive telephone counseling from specially trained FTC and contractor personnel to help them resolve problems that may have resulted from the misuse of their identities. In addition, the hotline phone counselors enter information from the consumers' complaints into a centralized database, the Identity Theft Data Clearinghouse. In operation since November 1, 1999, the Identity Theft Hotline has averaged over 400 calls per week.

Our aim with each consumer call is to provide the comprehensive information needed to guard against or resolve problems caused by identity theft, and to assist in streamlining the process for the consumer wherever possible. Although there is generally no way for consumers to avoid contacting the many creditors who may be

---

[17] 18 U.S.C. § 1028(a)(7). The statute further defines "means of identification" to include "any name or number that may be used, alone or in conjunction with any other information, to identify a specific individual," including, among other things, name, address, social security number, driver's license number, biometric data, access devices (*i.e.*, credit cards), electronic identification number or routing code, and telecommunication identifying information.

[18] Prior to the passage of the Act, financial institutions rather than individuals tended to be viewed as the primary victims of identity theft because individual consumers' financial liability is often limited. Setting up an assistance process for consumer victims is consistent with one of the Act's stated goals, to recognize the individual victims of identity theft. *See* S. Rep. No. 105–274, at 4 (1998).

[19] Pub. L. No. 105–318 § 5, 112 Stat. 3010 (1998) (codified at 18 U.S.C. § 1028 note).

[20] Most identity theft cases are best addressed through criminal prosecution. The FTC itself has no direct criminal law enforcement authority. Under its civil law enforcement authority provided by section 5 of the FTC Act, the Commission may, in appropriate cases, bring actions to stop practices that involve or facilitate identity theft. The practices the Commission expects to focus its law enforcement resources on are those where the effect is widespread and where civil remedies are likely to be effective. See, e.g., *FTC* v. *J.K. Publications, Inc., et al.*, No. CV 99–00044 ABC (AJWx) (C.D. Cal., Mar. 16, 1999) (order granting preliminary injunction) (alleging that defendants obtained consumers' credit card numbers without their knowledge and billed consumers' accounts for unordered or fictitious Internet services); *FTC* v. *James J. Rapp and Regana L. Rapp, individually and doing business as Touch Tone Information Inc., et al.*, Docket No. CV 99–WM–783 (D. Colo., filed April 21, 1999) (alleging that defendants obtained private financial information under false pretenses).

involved, our goal is that consumers should be able to make a single phone call to our hotline to report the offense, receive the information and assistance they need, and have their complaints referred to the appropriate government agency.

In particular, consumers who are victims of identity theft receive specific information about how to try to prevent additional harm to their finances and credit histories. The phone counselors instruct the callers to contact each of the three credit reporting agencies to obtain copies of their credit reports and request that a fraud alert be placed on their credit report.[21] We advise consumers to review the information on the credit reports carefully to detect any additional evidence of identity theft. The counselors also routinely inform callers of their rights under the Fair Credit Reporting Act and provide them with the procedures for correcting misinformation on a credit report. Consumers receive additional information telling them how to contact each of the creditors or service providers where the identity thief has established or accessed an account, and to follow up in writing by certified mail, return receipt requested. Where the identity theft involves "open end" credit accounts,[22] consumers are advised on how to take advantage of their rights under the Fair Credit Billing Act, which, among other things, limits their responsibility for unauthorized charges to fifty dollars in most instances. Consumers who have been contacted by a debt collector regarding debts left behind by the identity thief are advised of their rights under the Fair Debt Collection Practices Act, which limits debt collectors in their collection of debts.

In addition, the FTC phone counselors advise consumers to notify their local police departments, both because local law enforcement may be in the best position to catch and prosecute identity thieves, and because getting a police report often helps consumers in demonstrating to would-be creditors and debt collectors that they are genuine victims of identity theft. Almost half the states have enacted their own identity theft laws, and our counselors, in appropriate circumstances, will refer consumers to other state and local authorities, to pursue potential criminal investigation or prosecution.

(2) *Identity Theft complaint database.* As mentioned above, detailed information from the complaints received on the FTC's toll-free Identity Theft Hotline is entered into the FTC's Identity Theft Data Clearinghouse ("Clearinghouse"). The Clearinghouse is designed to become a comprehensive, government-wide repository of information collected from victims of identity theft. In the near future, it will begin incorporating complaints received by other government agencies, such as the Social Security Administration. Consumers can also enter their own complaint information via the public user complaint form at *www.consumer.gov/idtheft.*[23]

Having designed and built the Clearinghouse database itself, the Commission is now developing the tools to extract and analyze the information it contains.[24] The information collected in the Clearinghouse will provide the Commission with a better understanding of how identity theft occurs. In particular, we will look at whether certain types of transactions or business practices lead to greater opportunities for the theft of a person's personal information or facilitate the misuse of that information once obtained. As we begin to identify trends and patterns in the occurrence of identity theft, we will share this information with our law enforcement partners so that they may better target their resources.[25]

---

[21] These fraud alerts request that the consumer be contacted when new credit is applied for in that consumer's name.

[22] The Fair Credit Billing Act applies to "open end" credit accounts, such as credit cards, revolving charge accounts, and overdraft checking accounts. It does not cover installment contracts such as loans or extensions of credit that are repaid on a fixed schedule.

[23] See page 14, *infra.*

[24] While Congress authorized the appropriation of such sums as may be necessary to carry out the FTC's obligations under the Identity Theft Act, Pub. L. No. 105–318 § 5(b), 112 Stat. 310 (1998), no funds have been appropriated for the Commission's identity theft program. Our ability to fully build out our database, including making the information contained therein electronically available to our law enforcement partners, as well as our ability to perform sophisticated analyses of the data we collect, is contingent on the appropriation of adequate funds. Our budget requests for the next three years ask for funding of $2.8 million to complete the development of the system and maintain our call handling and consumer education responsibilities. Appropriations at the requested level would enable us to handle 100,000 calls for fiscal year 2001, and 200,000 annually thereafter. We have, in addition, submitted a reprogramming request to provide $625,000 in funds for fiscal year 2000. Of this request, which is now pending with the Appropriations Subcommittees, $525,000 would be distributed to the agency's contract account, and $100,000 to our equipment account.

[25] In addition to our collaborative work with our law enforcement partners, the Commission is looking for opportunities to work with private sector entities who are critical to addressing identity theft issues. For example, credit reporting agencies could provide substantial assistance

Continued

Moreover, the Identity Theft Data Clearinghouse will be available to law enforcement agencies at the federal, state, and local level through a secure, web-based interface. The Commission expects that the Clearinghouse will allow the many agencies involved in combating identity theft to share data, enabling these offices to work more effectively to track down identity thieves and assist consumers.[26] Criminal law enforcement agencies could take advantage of this central repository of complaints to spot patterns that might not otherwise be apparent from isolated reports. For example, federal law enforcement agencies may be able to identify more readily when individuals may have been victims of an organized or large-scale identity theft ring.

In addition, the Clearinghouse will facilitate the referral process required by the Identity Theft Act. Building upon the Commission's experience in sharing data and making referrals to combat consumer fraud through its successful Consumer Sentinel network,[27] we envision making identity theft referrals in a variety of ways beyond simply referring individual callers to appropriate agencies. As mentioned above, Clearinghouse members will be able to access this secure database directly from their desktops in order to support their investigations. In addition, the Commission plans to disseminate complaint information through customized standard reports, extracting for our law enforcement partners the Clearinghouse complaints that meet the criteria they have designated. Finally, when, during the course of our own in-house data analysis, we identify trends or patterns in the data that appear to have ramifications for our law enforcement partners, we will notify them of that information. Numerous law enforcement agencies have already expressed an interest in receiving information and referrals in these ways.[28]

(3) *Consumer Education*. The FTC has taken the lead in coordinating the efforts of government agencies and organizations to develop and disseminate comprehensive consumer education material for victims of identity theft, and those concerned with preventing identity theft.[29] The results of the FTC's efforts include both print publications and a website, located at *www.consumer.gov/idtheft*. This collaborative consumer education effort is ongoing; we hope to lead a similar joint effort with many of the private sector financial institutions that have an interest in preventing and curing the effects of identity theft.

The FTC's most recent publication in this area is a booklet entitled: *Identity Theft: When Bad Things Happen to Your Good Name*.[30] The 21-page booklet covers a wide range of topics, including how identity theft occurs, how consumers can protect their personal information and minimize their risk, what steps to take immediately upon finding out they are a victim, and how to correct credit-related and other problems that may result from identity theft. It also describes federal and state resources that are available to consumers who have particular problems as a result of identity theft. In addition to our own initial distribution of this booklet, the Social Security Administration has ordered and plans to distribute 100,000 copies of the booklet. The Federal Deposit Insurance Corporation has also indicated that it will print and distribute the booklet.

The Identity Theft web page features a web-based complaint form, allowing consumers to send complaints directly into the Identity Theft Data Clearinghouse. The website also includes the comprehensive identity theft booklet as well as other publications, tips for consumers, testimony and reports, information on recent identity

---

by detailing for this project how their existing fraud operations and databases function, and how information could most efficiently be shared with them.

[26] The Commission has successfully undertaken a similar effort with respect to consumer fraud. The FTC's Consumer Sentinel network is a bi-national database of telemarketing, direct mail, and Internet complaints accessible to law enforcement officials throughout the U.S. and Canada. Currently the Sentinel database contains more than 210,000 entries, and is used by more than 200 law enforcement offices, ranging from local sheriff's offices to FBI field offices.

[27] See *supra* note 26.

[28] Pursuant to the requirements of the Identity Theft Act, the FTC hopes to gain the cooperation of the three major credit reporting agencies to establish an analogous information sharing and referral system to allow us to refer complaints received on our toll-free number to individual credit bureaus for assistance or resolution, as appropriate.

[29] Among the organizations the FTC has brought into this effort are the Federal Reserve Board, the Office of the Comptroller of the Currency, the Federal Deposit Insurance Corporation, the National Credit Union Administration, the Office of Thrift Supervision, the Department of Justice, the U.S. Secret Service, the Federal Bureau of Investigation, the Postal Inspection Service, the Internal Revenue Service, the Social Security Administration, the Federal Communications Commission, the Securities and Exchange Commission, the U.S. Trustees, and the National Association of Attorneys General.

[30] In April, 1999 the FTC took the interim step of issuing a consumer alert, *Identity Crisis * * * What to Do If Your Identity Is Stolen*, which gives consumers an overview of what to do if they are victims of identity theft.

theft cases, links to identity theft-related state and federal laws, descriptions of common identity theft scams, and links to other organizations and resources.[31]

Finally, the Commission recognizes that the success of this effort hinges on the public's awareness of these resources. On February 17, 2000, the Commission announced its Identity Theft Program, promoting the toll-free number, the website and our consumer education campaign.[32] We anticipate that we will see an increase in our call volume and website visits following these efforts to raise the public awareness of identity theft.

IV. ONGOING ISSUES

In May 1998, the Commission testified before this subcommittee in support of the Identity Theft and Assumption Deterrence Act. The Commission continues to believe that the Act is an important tool in addressing the problem of identity theft. Since its passage, the FTC has increased its efforts to develop a program to quantify the data regarding identity theft, to provide assistance to identity theft victims who seek help in resolving identity theft disputes, and provide consumers and others a central place in the federal government to go for information about identity theft. Already, in the relatively brief time our identity theft hotline has been operational, the FTC has assisted over 4000 consumers who have been, or are worried about becoming, victims of identity theft. We anticipate that our consumer assistance program will continue to expand and grow over the coming months.

Notwithstanding our efforts and those of other law enforcement agencies, however, identity theft continues to pose significant problems for consumers. Some preliminary areas of concern to the Commission are as follows:

Prevention. Although many bank, credit card issuers, and other companies have put into place extensive systems to guard against identity theft, there nonetheless remain a number of continuing practices that may contribute to the problem of identity theft. Fraud alerts, for instance, are not fulproof. Identity thieves may be able to open accounts in the victim's name notwithstanding a fraud alert either because the fraud alert is not picked up by the credit scoring or other automated system used by the new creditor, or because the creditor fails to take sufficient precautions to verify the applicant's legitimacy when presented with a fraud alert. One caller to the FTC's hotline whose wallet had been stolen, for example, reported that *after* placing a fraud alert on her credit reports, at least seven fraudulent accounts were opened in her name at various retail establishments that granted "instant credit" based only on a credit score that did not take into account fraud alerts.[33]

In addition, although individual credit issuers have systems to detect automatically unusual patterns of activity, it is more difficult to detect unusual activity across creditors. Thus, for example, if an identity thief opens 30 different credit accounts in the course of 2 days, none of the 30 individual creditors may notice anything unusual. However, taken as a whole, the pattern of activity would likely trigger suspicion. Thus, one possible area for further action lies in bringing together creditors and credit reporting agencies (the group that is probably best placed to notice when there have been numerous credit applications or new accounts opened) to develop mechanisms for detecting such fraud—and thus heading off identity theft.

Remediation. Identity theft victims continue to face numerous obstacles to resolving the credit problems that frequently result from identity theft.[34] For example,

---

[31] The *www.consumer.gov* site is a multi-agency "one-stop" website for consumer information. The FTC hosts the server and provides all technical maintenance for the site. It contains a wide array of consumer information and currently has links to information from 61 federal agencies. The consumer.gov project was awarded the Hammer Award in March 1999.

[32] While the toll-free number has been operational since November 1999, we waited several months to make a major announcement in order to fully train the telephone counselors, and otherwise smooth out the data collection operations. Even without a formal announcement, the toll-free line has received an average of 400 calls per week.

[33] Of course, it is important to the prevention of identity theft that creditors pay attention and follow-up with appropriate verification procedures wherever there are possible indicia of fraud. One Arlington, Virginia resident who called the FTC had been disturbed to find that her ATM card no longer worked. When she called her bank, she learned that someone using her name had reported her card lost, and asked that a replacement card be sent—to Brooklyn, New York. The sudden change-of-address presumably should have raised a red flag, but, in fact, apparently triggered no further investigation. Such oversights, often committed out of an understandable desire to provide prompt customer service, do not appear to be uncommon.

[34] Some identity theft victims face significant, non-credit-related problems as well. For example, in a small but troubling number of cases, consumers calling the FTC's toll-free number have reported that they themselves have been arrested because of something an identity thief did while using their name, or that they learned they had a criminal arrest or conviction on record

Continued

many consumers must contact and re-contact creditors, credit bureaus, and debt collectors, often with frustrating results. Using the data collected from consumer complaints, the Commission is actively monitoring the nature and extent of problems reported by consumers, and looking at possible means of addressing these problems, including ways of streamlining the remediation process.

In particular, the FTC believes that, as a first step, it would benefit consumers if they could make a single phone call—presumably, to any of the major credit bureaus or to the FTC's hotline—and have a fraud alert placed on all three of their credit reports, and copies of each of their three reports sent to their home address. The success of such an effort depends on the cooperation of the major credit bureaus.[35]

As the FTC's new identity theft program expands, the Commission will have more data and experience from which to draw in determining what additional actions may need to be taken to best assist identity theft victims.

V. COOPERATIVE EFFORTS

The Commission has been working closely with other agencies in a number of ways to establish a coordinated effort to identify the factors that lead to identity theft, work to minimize those opportunities, enhance law enforcement and help consumers resolve identity theft problems. In April 1999, for example, Commission staff held a meeting with representatives of 17 federal agencies as well as the National Association of Attorneys General to discuss implementing the consumer assistance provisions of the Identity Theft Act. In addition, FTC staff participates in the identity theft subcommittee of the Attorney General's Council on White Collar Crime, which has, among other things, developed guidance for law enforcement field offices on how best to assist identity theft victims. FTC staff also coordinates with staff from the Social Security Administration's Inspector General's Office on the handling of social security number misuse complaints, a leading source of identity theft problems.

Furthermore, almost half of the states have now enacted their own statutes specifically criminalizing identity theft. Others have passed, or are considering, further legislation to assist victims of identity theft,[36] including legislation specifically designed to help victims clear up their credit records.[37] The Commission is committed to working with states and local governments on this issue, and learning from their efforts.

Most recently, FTC staff has been assisting the Department of Treasury on plans for the upcoming National Summit on Identity Theft on March 15–16. The Summit provides a significant opportunity for government and business leaders to develop partnerships to combat identity theft and assist its victims.

VI. CONCLUSION

The Commission, working closely with other federal agencies and the private sector, has already made strides towards identifying ways to reduce the incidence of identity theft. More focused law enforcement, greater consumer education and increased awareness by the private sector will all contribute to this effort. The FTC also looks forward to working with the Subcommittee to find ways to prevent this crime and to assist its victims.

Senator KYL. Thank you very much. I appreciate the testimony that both of you have given to us.

---

because an identity thief used identification with their name rather than his or her own when arrested for committing some other crime. Needless to say, correcting legal arrest or conviction records can prove extremely difficult.

[35] Another question potentially raised by the experiences of identity theft victims is whether the protections currently afforded by laws such as the Fair Credit Reporting Act and Fair Credit Billing Act are adequate for resolving the problems commonly faced by identity theft victims. Because the data the Commission has gathered in the short time its hotline has been operational are limited, it would be premature to try to resolve such questions at this time.

[36] *See, e.g.,* Iowa Code § 714.16B (creating a private right of action for victims of identity theft).

[37] *See* Cal. Civ. Code § 1785.6 (providing that if a consumer provides a credit bureau with a copy of police report of identity theft, the credit bureau "shall promptly and permanently block reporting any information that the consumer alleges appears on his or her credit report as a result of a violation of Section 530.5 of the Penal Code [the California identity theft statute] so that the information cannot be reported"; the information may be unblocked "only upon a preponderance of the evidence" establishing that the information was blocked due to fraud, error, or that the consumer knew or should have known that he or she obtained goods, services, or moneys as a result of the blocked transactions).

Let me just get right to the heart of a couple of questions I had regarding the FTC. Have you been appropriated enough money, do you think, to accomplish the various tasks that the statute mandates to the FTC? If not, is there anything else that you need?

Ms. BERNSTEIN. We really haven't been appropriated any money for this program. What we have done so far in my bureau is shifting funds from other programs to try to staff, as we have, this program, and I think we have done well. However, we have a pending reprogramming request for $625,000 for the current fiscal year, and the Commission submitted a budget that requested $2.8 million for each of the next 3 years. We have estimated that if the reprogramming request was granted and the new budget put in place that we would be well provided for in terms of resources to be able to run a really more aggressive program.

Senator KYL. Was that the budget request from the White House?

Ms. BERNSTEIN. Yes.

Senator KYL. OK, good, and if you need help on the reprogramming, too, be sure and let us know about that.

Ms. BERNSTEIN. Thank you.

Senator KYL. Have the credit bureaus been working, do you think, well with the FTC to address the problem generally?

Ms. BERNSTEIN. With every effort to be diplomatic, I would say that we would have hoped for more cooperation.

Senator KYL. I kind of thought so. What about a special number? And I am not suggesting that the Federal Government mandate this, but considering one of Ms. Mitchell's problems, do you think that if we encouraged the credit bureaus to have a special number for ID theft reporting that people wouldn't have as much trouble getting through to a real person to talk about these things?

Ms. BERNSTEIN. I would think that that would be a great assistance to people. Just one central source, whether it be to the FTC or whether they do it separately, any way, as Maureen said, that you could cut down on the number of efforts that the individual has to make would be extremely helpful.

Senator KYL. Any recommendations that you would like to make to us in that regard I would appreciate very much, not necessarily as amendments to the existing law, not necessarily law, but recommendations that we might implement by encouraging credit agencies to do certain things or in some other way effectuating them. That would all be appreciated.

With respect to local law enforcement, one of Ms. Mitchell's concerns was that they didn't seem to be as aware of the Federal law as they need to be. What more can we do to get notice—and maybe this is a question really for both of you—notice more to the local law enforcement agencies?

Mr. REGAN. Yes, sir. We try to address that through our task force involvement. We have currently 28 task forces throughout the country and they include State, local and county police officers. Unfortunately, we are comparatively a small agency. So our task forces aren't in every city, but where they are we include all law enforcement agencies in that area and we try to get it out like that.

We also have an Internet site, on which we put several things out there now. In fact, we see the future of identity theft basically

being on the electronic side. We are moving toward a cashless society, or an electronic commerce type society ourselves here in the United States, and we are seeing most of the crime activity being used within the Internet, either the Internet being used as a tool to move it forward or to hide behind it, to be anonymous, and so forth.

Identity theft is a component of what is going on there. The theft of people's account numbers through Internet hacking and through skimming, which is the theft of account information off the back of mag strips, are all part of it. And one of the things we are doing with local law enforcement—and I think you have a copy of it, sir—is we printed this up for local law enforcement and it is called ''Best Practices for Seizing Electronic Evidence.''

And what this is for is to give the local police officer, who is usually the first responder, because, like I say, we are a comparatively small agency—if there is a problem, the local police officer is the first one on the scene. And if, in fact, it is an identity theft where they use the electronic medium, what is that police officer supposed to do with that computer? And it is supposed to make him a little bit comfortable in what could be considered evidence within that area, what holds information, what would hold account numbers in people's names, and so forth, and how to safely handle it, as well as a list of contacts and how to track back e-mail headers, and so forth.

So we are doing certain things like that as outreach to the field now, and we continue to do it. This is also available on our Internet site for those agencies we haven't gotten the booklets to yet. We have distributed over 60,000 of them this year, and we are hoping to do another 100,000 by the end of this coming year.

Senator KYL. I might suggest that maybe there be some reference also when you do this again to the Federal law so that they can appreciate the fact that there are both Federal and State laws involved. This looks very helpful, by the way.

Mr. REGAN. Yes, sir, thank you.

Senator KYL. My understanding is that what has happened is since we got the law passed that a lot of people are now being charged under this new law, but that we might not be aware of the true magnitude of the crime because there are a lot of plea bargains taken, and that frequently the new law is the charge that is dropped in the course of making the plea bargain.

It is obviously helpful to have that additional crime to charge because you can more likely get a plea bargain and a better sentence, but frequently this is the particular charge that is dropped. So we may not have a real good handle on the number of situations in which people have actually been guilty of this particular crime.

Can you discuss that with us at all at this point?

Mr. REGAN. Yes, sir. I think you are a hundred percent correct. I think this law is used extensively in financial crimes. It would be virtually impossible to perform most financial crimes without some form of false identification, not necessarily an identity theft, but some form of false identification.

When you talk about credit fraud, it is usually an identity theft. When you talk about skimming, it would be an identity theft. And what all too often will happen is we will pick up an individual and

that individual might be indicted on 15, 20 counts. And the agreement comes out that they take a plea to certain counts, maybe a bank card count or a credit card count. And the other counts, although they were all part of the indictment, just fall off by the plea, so that it is very hard to capture that information that comes through. But I think that this violation is used extensively in Federal financial criminal investigations, sir.

Senator KYL. Well, we will, of course, want to continue to follow the progress of that to make sure that what we have done is worthwhile for law enforcement agencies. And if there are any changes that need to be made in it, we can, based on your recommendations, make those changes.

Are you getting the information you need from the FTC for the Secret Service to initiate an investigation when it is warranted?

Mr. REGAN. Yes, sir, very much so. In fact, we are working very, very closely with the FTC and it is working out very well. In fact, I have worked with Beth Grossman myself on numerous occasions and it is a pleasure to work with them on this.

Ms. BERNSTEIN. Mr. Chairman, I may mention in connection with the local law enforcement question that you asked that we think that when the identity theft clearinghouse is really fully established for the benefit of local law enforcement—that has been our experience with our database that that is just a boon to a local law enforcement person. When he or she gets a call and is perhaps in a small community somewhere and doesn't have a lot of assistance to be able to dial into that database and quickly find out whether there have been other complaints about that particular theft, what has happened with it, where they can get assistance, it has just been an enormous help in other fraud areas that we have used. So when we are up to the place where it is fully developed—and we are not too far from that—I think it will be an enormous assistance to local law enforcement.

Senator KYL. That is great. That is one of the two directions we want to go. Let me focus on the other direction, and that is how to make the system more user-friendly and effective for the actual victims, people like Ms. Mitchell.

Maybe you could walk us through what happens when somebody like Ms. Mitchell calls the FTC hotline. What do you do? And then more specifically, how is that helping her to both prevent continual violations of her identity or credit and cleaning up the credit violations that have already occurred?

Ms. BERNSTEIN. Well, the first thing that happens is Ms. Mitchell, for example, would call and in this case Kathleen Lund answers the telephone. And I would say that we have specially trained those counselors who are dealing with identity theft because it is more complicated; it is criminal as opposed to other types of fraud which are often civil, as you know. And we have worked hard to be sure that we were providing the counselors with enough information so that they would know how to proceed.

And Kathleen would then ask her what happened, obviously, and she would tell her, get the relevant information about it. And then the first thing to do would be to advise her of what steps she ought to take immediately, and those steps, of course, are, as you heard from Ms. Mitchell, to notify the credit bureaus, to notify creditors,

the merchants that she talked about, and most particularly to call the police. It is important to have a police report on record very quickly.

She would then provide her with fuller information, which she can get on a Web site or we would put into the mail, whatever is convenient for her, to begin the process of getting those fraud alerts on the credit reports because that is the first line of defense.

Senator KYL. Now, how, physically, does that actually occur?

Ms. BERNSTEIN. How physically does it occur?

Senator KYL. Yes. She has now notified the FTC.

Ms. BERNSTEIN. The FTC tells her the numbers of the credit bureaus, and there are three of them, as she indicated, and they have a line that we ask her to call because that is what the process is. She then calls the credit bureau—and hopefully she doesn't get a ringing phone; hopefully, she gets a real person—and reports what has happened to her and asks them to immediately put a fraud flag on her credit report.

The purpose of that obviously is to alert others—merchants, the fellow who is going to issue a loan for a car—when he or she asks for a credit report, which they do before opening a line of credit, to see that there is already a fraud alert on that credit report. That really should be a warning to that creditor to think carefully before extending credit to what may not be the appropriate person. So, that is how that gets done.

Now, Ms. Mitchell's experience was, I think—and she made a valuable point about it—if it is on the last page of the credit report and it is in type that doesn't jump out at the person who is reviewing it and they are in a hurry, it certainly would be an improvement—and it doesn't have to be by Federal law; it could certainly be something that the committee could encourage the credit bureaus to undertake voluntarily to improve the fraud alerts that are on the credit reports.

Senator KYL. How do you at the FTC, or the credit bureaus themselves, verify the validity of the information presented by somebody such as Ms. Mitchell so that they know that it is not a scam themselves?

Ms. BERNSTEIN. Well, we have some ways of verifying who the person is. We can communicate back with them. They give us an address. We can check them out as to whether or not we have other indications of who they are. We have not experienced getting false claims into our system. That would be something that we would be careful with, obviously, before we proceed.

The credit bureaus also have their regular means of verifying who people are that they have to do all the time because they are issuing credit reports. So they have various means of verification, like drivers' licenses and other documentation that they can ask for before proceeding.

Senator KYL. I think one thing that has occurred to me is that maybe we need to ask some of the credit agency or credit bureau people to come and testify to us, and we can present some concerns and questions to them and maybe they can tell us what they might do to improve the situation. Do you think that might be a helpful exercise?

Ms. BERNSTEIN. I think it would be very helpful.

Senator KYL. OK, I think we will consider doing that. Would it be possible to accomplish this notification electronically through the FTC, do you think?

Ms. BERNSTEIN. You mean a generalized notification to the credit bureaus?

Senator KYL. Yes.

Ms. BERNSTEIN. Yes, I think so; I think it could be.

Senator KYL. In other words, Ms. Mitchell has notified us. We have determined, at least prime facie, that there is a valid complaint on her part. Would the three of you please verify this independently and flag it, if appropriate?

Ms. BERNSTEIN. Right, and let us know that it has been verified or it has been flagged.

Senator KYL. Would you consider doing that and get back to us to see how easy that would be, or difficult?

Ms. BERNSTEIN. I would be glad to do that, and I would need to see how easy it is to do.

Senator KYL. Yes.

Ms. BERNSTEIN. But Beth here is almost as good on computers as the thieves are, and she will be able to tell me.

Senator KYL. Single-handedly.

Ms. BERNSTEIN. Single-handedly is right.

Senator KYL. Well, check that out as an additional way maybe to get this process undertaken.

Ms. BERNSTEIN. We would be glad to explore that, or perhaps there is another way that that would be useful, and we will be glad to respond to that.

Senator KYL. Well, I think what I am getting at here for both of you is, first of all, to compliment both of you for helping us to use the law that we passed, to confirm that we are on the right track, that it seems to be a positive development in the area. It obviously doesn't solve the problem, but it can make life a little easier for those whose identity has been stolen, and at least help you also to go after the perpetrators.

What we would like to do is to get any other suggestions that either the Secret Service or the FTC have as additional experience shows you what is working and what isn't working, either to modify your internal operating procedures or perhaps to give us additional suggestions as to what we should do with the law.

I would also ask on behalf of my colleagues on the committee to get the data together in whatever good, reportable form you are comfortable with and get that to us as soon as you can so that we can report to our colleagues how it is working and what changes may be needed—and we will call on you to determine what the best reportable form for that is and when you can get that data to us—and then finally any suggestions that you would have about any additional hearings, including perhaps the credit agencies.

And I would suggest would it not be appropriate not only to have credit bureaus, but also a couple of the larger credit-extending agencies? I don't want to pick on anybody in particular, but one of the major automobile manufacturers and sellers of automobiles extending credit, somebody like that. We will work with you so that you can give us some suggestions as to maybe the most representative of that kind of entity.

There was one other thing in my mind and now it has flown out. Well, any other suggestions from either of you as to what the committee should be doing at this point in our continuing oversight? Anything else from either of you?

[No response.]

Senator KYL. What will you be doing, either or both of you, at next week's seminar, and can you describe for us briefly how that will occur and what the public might expect from that, how they could tune in and participate. This is the President's symposium or whatever it is called.

Mr. REGAN. Yes, sir. As far as the Secret Service and myself in particular, I will be chairing one of the committees addressing law enforcement and our response to it, and more importantly how do we respond both nationally and internationally, because one of the things we are seeing on the identity theft issue today is there is no such thing as a case here in, say, Washington, DC.

What we will see is they are organized and they are rings, as we heard earlier, and they are often both national and international in scope. A lot of things we are dealing with are on the international side of the house on how to deal with countries in the G–8 with law enforcement issues over there, how to identify points of compromise.

One of the questions that Senator Grassley brought up, did you ever find out how your point of compromise came about—well, it is very difficult at times when you are dealing with a multitude of different ways for your identity to be stolen. Some of the Nigerian organized criminal groups are very, very good at recruitment of individuals from banks and from private industry, and so forth, to get background information. The Chinese gangs have moved into the electronic age where they are using hacking devices and Internet theft to actually get into it.

So we are trying to identify how points of compromise come about and shut them down. More importantly, how can law enforcement respond, especially as the technology moves forward and electronically everyday it just enhances. You know, today's computer equipment is really obsolete 6 months down the road, and that is kind of what we are looking at.

Because we are going to an electronic commerce society, the United States becomes a huge pool of potential victims because we all have credit now. You know, 5 years ago who would have thought that you could go to a gas station, take your debit card and fill up your car and never see the attendant? People don't even get their paychecks anymore; they are electronically deposited into their accounts.

So we are moving away from paper and we are moving toward electronics, and it is a good thing. But with all this enthusiasm for the Internet, you have got to temper it with a little caution. We are seeing the same tools that are being used to make our lives a little better are also being used to defraud financial institutions and steal people's identities.

Senator KYL. So you will be participating in the program?

Mr. REGAN. Yes, sir.

Senator KYL. Ms. Bernstein, before you answer, let me just for the benefit of the audience make something kind of clear here. This

subcommittee of the Judiciary Committee is the Subcommittee on Technology, Terrorism, and Government Information. And it is not always the case that all three of those things intersect, but at least two of the three intersect here. Government information could, as a result of Social Security numbers and other information, be involved as well.

The charge for our subcommittee is to try to keep track of the evolution of technology and how law needs to keep pace with that evolution. A couple of other examples: cell phone cloning didn't exist 10 or 12 years ago. It all of a sudden got to be a big crime and we needed to bring the law with respect to cell phone cloning up to date. We are trying to do the same with Internet gambling. Activity that has been prohibited since 1961 under the Federal Wire and Telephone Act, we suddenly find may be somewhat outdated as a result of the difference in the transmission of the data. So the Senate unanimously passed revisions to that law.

And there will be other efforts, including this identity theft, which isn't necessarily dependent upon electronic transfer of data or hacking into a computer system to get the information. Sometimes, it is as simple as going through a garbage can, but it is usually still pulling off a slip that has to do with some credit card or something else that is transmitted electronically, but not necessarily always.

So, that is what our subcommittee is all about, and it takes the efforts of entities like the FTC and the Secret Service to help us do our job. So for anybody that is concerned or interested in that, you are welcome to contact our staff for further information. Or if you have some suggestions about other things we need to do, we would be happy to take those, too.

Finally, Ms. Bernstein, what will your participation be in this meeting next week?

Ms. BERNSTEIN. Mr. Chairman, two of us are on panels. I am participating on a panel that is going to take some further initiatives for public-private partnerships for consumer education. Some of the things we have talked about today undoubtedly will be raised, and the private sector folks, I believe, will be attending and will participate on the panel. So we hope to get some commitments, if you will, from the private sector. We have in the past, and we are optimistic.

Hugh Stevenson, who is also on our staff, is on a panel that will be discussing additional ways to be of assistance to victims. That is something that you addressed, I know, in connection with the sponsorship of the legislation itself. And while we believe we have done a good job of training counselors to do a certain amount, there may be some other ways in which we can provide, either with other Government agencies or with the private sector, better ways to assist victims because it is such a difficult, difficult thing to undertake.

Senator KYL. I would especially be interested in the conclusions in that regard because I still don't think we have gone far enough in being able to help somebody like Ms. Mitchell actually go back and clear her credit.

Ms. Mitchell, could you come to the dias for one last question here that I neglected to ask before?

My question is this. What would be helpful to you that you don't currently have to help you clear your credit or to prevent entities from extending credit to the people who have stolen your identity? Once you know, in other words, that it has occurred and you have contacted the FTC and now you have got to go about the job of getting your credit cleared and stopping any further violations, what would be useful for you to have, if anything, to do that?

Ms. MITCHELL. I think there would be two things that would be very helpful. One would be the fraud alerts appearing on the credit reports in a very conspicuous place.

Senator KYL. Right, we got that.

Ms. MITCHELL. The other would be once it is established that a victim is a bona fide victim with whatever system of verification needs to be there, then one package of boilerplate documents to be filled out, a protocol that is universally accepted by all of the merchants who have been defrauded, rather than having the victim fill out 20 or 30 different protocols.

Senator KYL. Excellent. Now, what I would like to suggest, Ms. Bernstein, is when you meet with these folks next week, put that to them, because this would be better done voluntarily than through a law.

Ms. BERNSTEIN. We agree.

Senator KYL. See if they are willing to work on this problem with you and develop this protocol, and also more clearly and forthrightly post the fraud alert on their credit reporting. Maybe if you could get back to us after that or after you have had some contact with them, contact our staff so that we can see what we need to do, maybe calling them before us to see whether they are agreeable to these things, perhaps getting a report back from you. Most especially, we want to be able to report back to Ms. Mitchell.

So if there is nothing else that the three of you have, I will declare this meeting adjourned, but I thank you very, very much for joining us today. It has been very, very helpful.

Mr. REGAN. Thank you, Senator.

Ms. BERNSTEIN. Thank you.

Senator KYL. The hearing is adjourned.

[Whereupon, at 3:20 p.m., the subcommittee was adjourned.]

APPENDIX

QUESTIONS AND ANSWERS

RESPONSES OF JODIE BERNSTEIN TO QUESTIONS FROM SENATOR FEINSTEIN

Question 1. It is my understanding that the identity theft victim bears the responsibility for correcting errors on her credit record even after reporting the theft to the major credit bureaus and having a fraud alert placed on her file. For example, it is typically up to the identity fraud victim to call the affected creditors individually and alert them to the fraudulent activity in her name.

This task can be incredibly burdensome. There is no standardized form to report identity theft, so the victim must fill out multiple sets of forms with the same information. Despite months of effort and hundreds of phone calls, victims still report not being able to get their credit rating restored.

Do you think more can be done to assist identity theft victims who are trying to restore their credit rating? Is it possible to draft a single, standardized set of documents that victims could fill out?

Answer 1. We believe that more can, and should, be done to assist victims of identity theft restore their credit standing, and the Federal Trade Commission is working with other public and private organizations to identify the most effective ways to accomplish this. Many of the identity fraud victims who call the FTC's Identity Theft Hotline report their frustration at having to fill out numerous and different forms, and make a series of telephone calls in their attempt to resolve their identity theft-related disputes. Certainly, a single standardized affidavit, accepted by the credit reporting agencies ("CRA") and major financial and credit granting institutions, would relieve some of this burden and streamline the complaint process. As I noted in my testimony before the Subcommittee, we would support such an effort, and are ready to work with industry to develop a form that would meet the needs of the affected institutions.

A standardized form is just one measure that would relieve the burden on identity theft victims. Another practical step to streamline the complaint process would be to reduce the number of telephone calls the consumer has to make to report identity theft. Currently, an identity theft victim must contact each of the three major CRA's to request that a fraud alert be placed on her credit report. We would welcome a system that allowed a victim to call one of the agencies, and for that agency to transmit the information to the other two CRA's. In addition, some consumers learn only after calling our hotline that they should alert the CRA's if they are victims or potential victims of identity theft (*e.g.* if their wallet was lost or stolen). Assuming the availability of appropriate funding, we are prepared to establish the technology that would, with the consumer's consent, transmit the data to the CRA's to enable them to place a fraud alert on the credit report and send the victim a copy of their credit report, thus eliminating the need for the consumer to call the CRA's. We have raised this idea with representatives for the industry, and will move forward as soon as we obtain an indication of their willingness to pursue this system.

Question 2. What is your best estimate of the annual number of victims of identity fraud in this country? What is your best estimate of the annual financial costs of identity fraud to American consumers and American industry?

Answer 2. To the best of our knowledge, no current reliable statistics exist on the overall extent of identity theft in this country. From the limited available information, however, we estimate that there are hundreds of thousands of identity theft victims annually. According to the General Accounting Office's May 1998 report on

identity fraud (which, too, found no comprehensive statistics on identity fraud), Trans Union, one of the nation's three major credit bureaus, reported that they received over 500,000 calls to their fraud victim assistance department in 1997, approximately two-thirds of which involved incidents of identity theft. Government agencies, too, have heard from significant numbers of identity theft victims. In 1999, for example, the Social Security Administration's Office of Inspector General received 39,000 consumer complaints of "social security number misuse," a category generally equivalent to identity theft. The FTC, for its part, has recently received as many as 1,000 calls per week to its recently launched toll-free Identity Theft Hotline, and we believe that so far we are hearing from only a small minority of all identity theft victims.

As to the financial costs of identity theft, the Treasury Department has estimated that credit card fraud alone results in $2–3 billion dollars in fraud losses annually.

Question 3. In your testimony, you describe the practice of "skimming" in which identity thieves use sophisticated devices to intercept personal information on credit cards and ATM cards. How widespread is this practice? What can be done to stop this practice?

Answer 3. The Commission is very concerned about the practice of skimming and its implications for identity theft, but, as a civil law enforcement agency, lacks firsthand knowledge about the extent of this criminal practice. The American Bankers Association, however, has described skimming as the most significant problem facing the credit card industry today and in the near future. One important measure being taken to combat skimming—announced at the recent National Summit on Identity Theft—is the U.S. Secret Service's skimming database. Developed in partnership with the financial industry, the database helps identify common suspects and address trends in skimming and related financial crimes. We hope that this will serve as a model for ways in which the public and private sector can cooperate to thwart not only skimming but other fraudulent practices as well.

RESPONSES OF JODIE BERNSTEIN TO QUESTIONS FROM SENATOR GRASSLEY

Question 1. In your testimony, you referred to the Fair Credit Billing Act and the Fair Credit Reporting Act, and how these two laws provide important protections for consumers trying to clear up their credit records after having their identity stolen. Are statistics compiled by the FTC, or any other agency, to support whether these two laws are successfully aiding consumers? Do we know with certainty that consumer liability is limited and that credit reporting agencies are correcting inaccurate information?

Answer 1. As noted in our testimony, the Commission believes that the Fair Credit Billing Act and the Fair Credit Reporting Act provide important protections to consumers as they attempt to undue the credit damage done by an identity thief. Section 133 of the Fair Credit Billing Act (15 U.S.C. 1643) specifically limits liability of credit cardholders in the case of unauthorized use to $50. The Commission has received few complaints about companies not complying with this provision; indeed, it is our understanding that in most instances, credit card issuers waive the $50 charge and impose *no* liability on consumers for fraudulent credit card charges.

Section 611 of the Fair Credit Reporting Act (15 U.S.C. 1681i) requires consumer reporting agencies to investigate information in their files that is disputed by consumers as inaccurate or incomplete, and to delete or correct information based on the results of the investigation. Similarly, Section 623 of the Fair Credit Reporting Act (15 U.S.C. 1681s–2) requires credit information furnishers to reinvestigate information provided to credit reporting agencies that is disputed by consumers as inaccurate or incomplete and to report the results of that investigation to the credit reporting agencies. Because our identity theft database is still new, it is still too early for us to determine the extent to which the credit report inaccuracies that often result from identity theft are being promptly corrected by credit reporting agencies and credit information furnishers. We continue to monitor complaints from consumers on this issue. That the Commission is committed to enforcing the requirements of the Fair Credit Reporting Act is demonstrated by the FTC's recent actions against three major credit bureaus for failing to maintain toll-free telephone numbers with personnel accessible to consumers during normal business hours. Those actions were based on Section 609(c)(1)(B) of the Fair Credit Reporting Act, and were settled by an agreement filed on January 13, 2000, under which those credit bureaus paid civil penalties totaling $2,500,000.

Question 2. How do we know whether consumer information is provided only to entities with "permissible purposes?" Is that something we only find out when a consumer files a complaint?

Answer 2. Consumer complaints are a principle way we learn of consumer information being provided for impermissible purposes. Many of the complaints we receive come to us through the toll-free number connected with our Consumer Response Center, where our phone counselors enter them into our consumer complaint database. This data reveals individual cases of impermissible use of consumer information, as well as broader trends.

The Commission also learns of law violations through periodic reviews of industry business practices. For example, in the recent case against *Trans Union*, the Commission upheld the decision of an FTC administrative law judge, ordering Trans Union to stop selling consumer reports in the form of target marketing lists. The complaint had charged the sale of such lists violated the FCRA because the marketers to whom they were sold lacked a permissible purpose. The Commission had earlier entered into settlements with Experian and Equifax on similar charges.

Question 3. How many individuals have been prosecuted under the Identity Theft and Assumption Deterrence Act, since its passage in 1998, for knowingly transferring or using the identity of another person? How many have been convicted? Do you have any recommendations for changes in the identity theft law to enhance its effectiveness?

Answer 3. As you know, the Commission does not have jurisdiction to bring criminal prosecutions, and we do not have statistics on the total number of cases brought by the Department of Justice under the Identity Theft and Assumption Deterrence Act. The most recent data available to us, compiled by the U.S. Sentencing Commission, indicate that there were 12 criminal convictions under the Identity Theft and Assumption Deterrence Act in fiscal year 1999.

Such statistics may underestimate the number of recent identity theft cases for at least two reasons. First, because prosecutions under the Act may be brought only for crimes committed after the Act went into effect, there is necessarily a certain amount of lag time before convictions may be entered under the new statute. Second, identity theft is often part of a larger financial criminal scheme, and an identity theft prosecution may involve multiple counts under several different statutes; in a plea bargain one or more of these initial charges (including, in some instances, the identity theft charge) may be dropped.

We believe that at the present time law enforcement agencies have sufficiently little experience with the Identity Theft and Assumption Deterrence Act that it is therefore premature for us to make any recommendations for changes. As the FTC's Identity Theft Data Clearinghouse grows, however, and we have additional data available to us, we expect to revisit the issue of whether there are additional legislative measures that would more effectively combat identity theft and ensure that its victims are made whole.

Question 4. According to your testimony, it sounds like the centralized complaint and consumer education service has gotten underway only in the last few months. How long do you think it will take before you have the system in full operation?

Answer 4. The core elements of the centralized complaint and consumer education service were developed and implemented within the statutory one year period after passage of the Identity Theft and Assumption Deterrence Act in October 1998. While awaiting an appropriation to support the fuller development of the program, we have continued to build upon those core elements. The program's current operating components include:

- *Toll-free Telephone Number*

The FTC established a toll-free number, 1–877–IDTHEFT (1–877–438–4338), that consumers can call to report identity theft and receive guidance on the steps they can take to resolve credit and other problems that may have resulted from the identity theft. The number became operational on November 1, 1999.

- *Data Clearinghouse*

The FTC built and implemented the data collection functions of the Identity Theft Data Clearinghouse, a database to track identity theft complaints received by the FTC and other agencies. The database was launched in early November, in conjunction with the release of the toll-free number.

Since November 1, 1999, the Commission has continued developing the centralized complaint service in a number of ways. We have established basic data accessing and reporting capabilities, enabling the FTC to begin to analyze and identify trends and patterns in the consumer complaint information we collect. In addition,

the FTC has been meeting with the Social Security Administration's Office of Inspector General (SSA OIG) to establish mechanisms to download information obtained by the SSA Fraud Hotline into the FTC's Identity Theft Data Clearinghouse, as well as to refer complaints from the Clearinghouse to the SSA OIG's investigative staff. Finally, we have built the prototype for a web-based interface through which law enforcement agencies at the federal, state, and local level can access the Identity Theft Data Clearinghouse.

We added a public complaint form to the FTC's identity theft web site in mid-February. This form allows consumers to submit an identity theft complaint to the FTC via the Internet any time of the day or night. Consumers who use this form have access to all of the consumer education and referral material at the web site. In addition, their complaints go directly into the clearinghouse for analysis with the other consumer complaints about identity theft.

- *Consumer Education*

As the first step in our consumer education campaign, we developed a consumer publication entitled *Identity Crises * * * What to do If Your Identity is Stolen* that covers the basic steps victims should take when they discover that their identity has been stolen. We also revised a number of more targeted credit-related publications that may be of assistance to identity theft victims. In addition, by November 1, 1999 the FTC had established a web site devoted to identity theft issues at *www.consumer.gov/idtheft.* The web site contains tips for consumers, information on state and federal identity theft laws, recent cases and scams, links to other government agencies, and our consumer publications.

In addition, the FTC published a comprehensive booklet for consumers entitled *Identity Theft: When Bad Things Happen to Your Good Name,* which was released to the public on February 17, 2000. The booklet, which included contributions from over a dozen other government agencies, provides guidance on what to do to decrease the risk of identity theft; how to protect your personal information; the steps to take if you do become an identity theft victim; how to resolve credit problems that may result from identity theft; and who to contact in the government for assistance. I was pleased to be able to provide copies of this 21-page booklet, as well as other of our consumer education materials, to the Subcommittee at the time of my recent testimony.

The Commission achieved these accomplishments without yet receiving any appropriations earmarked for the Identity Theft Program. Additional steps to make the centralized complaint and consumer education service even more fully operational is dependent upon receiving necessary funding. There are several additional features that the Commission plans to add later this year if the agency receives approval of a pending $625,000 reprogramming request. Specifically, if funded, the FTC will make operational the web-based interface to provide direct access to the Identity Theft Data Clearinghouse by law enforcement agencies at the federal, state, and local level. With the receipt of necessary funding, the Commission would also be able to establish mechanisms to download into the FTC's data clearinghouse consumer complaint information gathered by other law enforcement partners, such as the Federal Reserve Board and the Office of the Comptroller of the Currency, thus enriching the data clearinghouse. The Commission would also further build out its data analysis tools to enable increased levels of review, analysis, and reporting on the data gathered through the complaint clearinghouse. This would permit us to identify categories of complaints suitable for referral to other law enforcement agencies for investigation or other action. The Commission would also develop automated mechanisms to make and track such referrals.

Question 4A. Has the FTC notified all law enforcement agencies to refer victims to the FTC hotline?

Answer 4A. From the outset, Commission staff has worked closely with all of the major federal law enforcement agencies that have a role in investigating and prosecuting identity theft. Representatives from these agencies are currently referring victims of identity theft to the FTC hotline. These agencies include the Department of Justice, the Federal Bureau of Investigation, the U.S. Secret Service, the U.S. Postal Inspection Service, and the Social Security Administration's Office of the Inspector General, as well as the banking regulatory agencies and other agencies with regulatory and policy-making functions. We are also working actively with the National Association of Attorneys General and the International Association of the Chiefs of Police and others to get word of our hotline out at the state and local level.

The Commission actively reaches out to federal, state and local entities to provide information on and more effectively combat identity theft. In April 1999, the FTC held a meeting with representatives of 17 federal agencies and the National Association of Attorneys General to discuss implementation of the consumer assistance pro-

visions of the Identity Theft and Assumption Deterrence Act, including design of the identity theft database and plans for producing and disseminating consumer education materials. In addition, among other efforts, we have been participating in ongoing meetings with the Department of Justice's Identity Theft Subcommittee of the AG's White Collar Crime Committee, the Office of the Comptroller of the Currency's Bank Fraud Working Group, and have attended various meetings of local law enforcement and business groups that focus on identity theft prevention and prosecution. Most recently, the FTC was a key participant in the Treasury Department's National Summit on Identity Theft. At each of these gatherings, FTC staff actively promote the toll-free number and database as part of our ongoing effort to make the database as comprehensive as possible.

Question 4B. Do you know if this (referral process) is happening?

Answer 4B. Yes, we do. For the past six weeks, we have been monitoring how callers to the FTC Identity Theft Hotline heard about our service. We have found that, on average, approximately 22 percent of the callers were referred to the FTC Identity Theft Hotline by local law enforcement or other government agencies. This is a significant source of referrals to our hotline. The remaining callers report having heard about the FTC's ID Theft Hotline from three basic sources: approximately 33 percent were referred by credit bureaus, banks and creditors; around 32 percent heard about the hotline from newspaper, television or radio reports; and about 9 percent learned about our hotline from friends or family members. (The remaining 4 percent were unable to specify the source.)

Question 5. What is the criteria used for referring complaints to the appropriate law enforcement authority?

Answer 5. As mentioned above, our referral function is not yet completely built and implemented, due to the need for additional funding. We therefore have not established firm automatic referral criteria. Ultimately the Commission envisions making identity theft referrals in a variety of ways, and the criteria will vary accordingly.

Currently, our phone counselors refer individual callers to appropriate agencies where those agencies or consumer assistance groups can offer real assistance to a caller with a particular problem. We also routinely refer callers to their local police to file a report, because we have found that even if the police are unable to investigate and catch the identity thief, having a police report can be of great assistance to the victim in clearing up the credit-related problems that may arise as a result of identity theft.

In addition, the Commission plans to disseminate complaint information through customized standard reports, extracting for our law enforcement partners the Clearinghouse complaints that meet the criteria they have designated. For example, as mentioned above, we are currently working with the Social Security Administration's Office of the Inspector General to establish specific criteria tailored to that agency's law enforcement priorities. We will provide the SSA OIG the information they want in the format and time frame they choose. Finally, when, during the course of our own in-house data analysis, we identify trends or patterns in the data that appear to have ramifications for our law enforcement partners, we will notify them of that information. Numerous law enforcement agencies have already expressed an interest in receiving information and referrals in these various ways.

Finally, we are designing systems so that our law enforcement partners can retrieve data directly from our database using their own desktop computers.

Question 6. I serve as Chairman of the Special Committee on Aging and, although I have a keen interest in the issue of identity theft in general, I have a real interest in whether elderly citizens are particularly vulnerable to having their identity stolen, as well. Will the FTC's centralized complaint database be able to collect information that will tell us the age group of the victims?

Answer 6. The database is able to reveal this information now. All information consumers provide to the FTC Identity Theft Hotline is strictly voluntary. Victims who call the hotline are asked for their date of birth. From its inception in November 1999 until March 31, 2000, approximately 52 percent of the callers have been willing to provide that information. Of the consumers who provided their age, about nine percent are age 65 and older. Approximately 26 percent were between the age of 45 and 64, inclusive. Approximately 39 percent were between 30 and 44 years old. Approximately 23 percent were between 19 and 29 years old, and less than three percent were age 18 and under.

Question 6A. Will it provide us with enough information to identify whether specific kinds of individuals are being targeted?

Answer 6A. Besides the consumer's address, with city, state, and zip code information, the database does not collect other types of demographic information. It does not, for example, collect information on the consumer's education level, type of employment, income level, or ethnicity. However, it does collect information on whether the victim has a relationship with the suspect. We have found that, through February 29, 2000, approximately 15 percent of the victims indicated that they had a relationship, such as a family, employment, or professional relationship, with the suspect.

○